Formal Methods for Interactive Systems

Part 7 — Task Failure and Behavioural Patterns

Antonio Cerone

United Nations University

International Institute for Software Technology

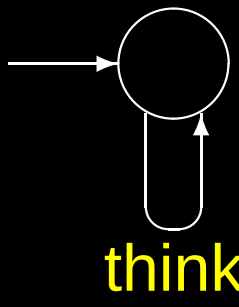
Macau SAR China

email: antonio@iist.unu.edu

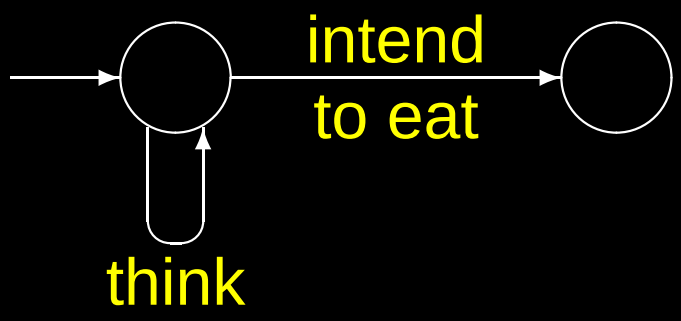
web: www.iist.unu.edu

Dining Philosopher

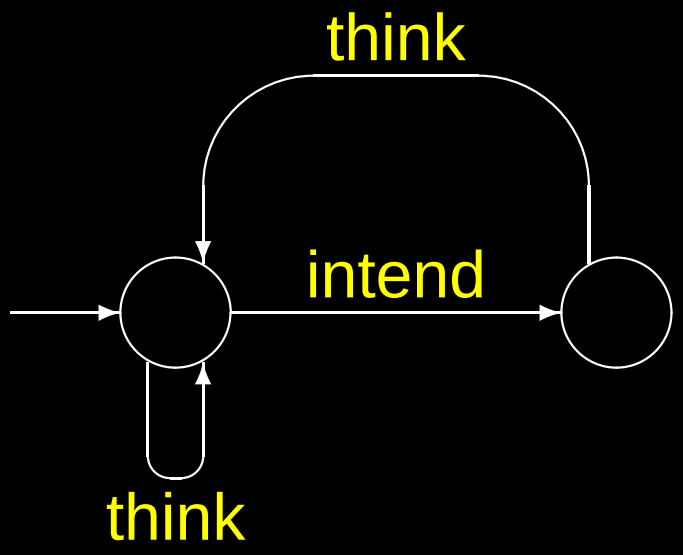
chopstick version



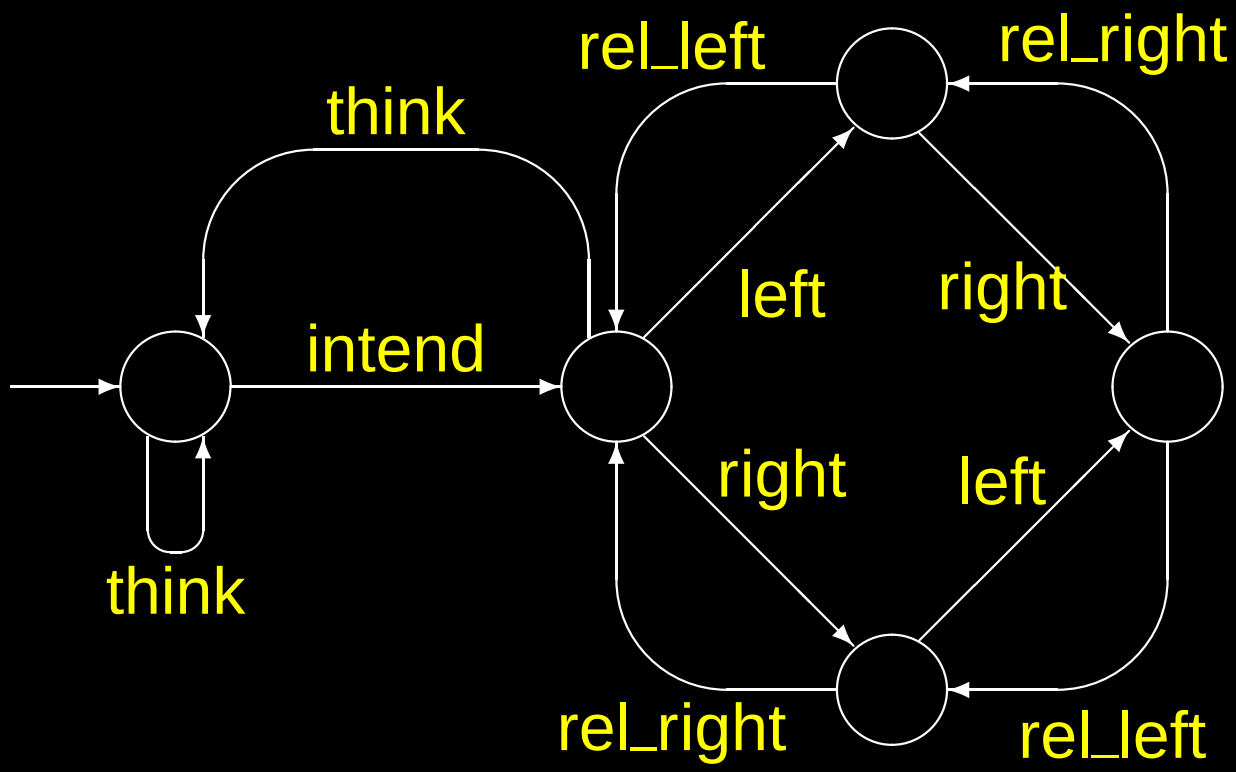
Dining Philosopher



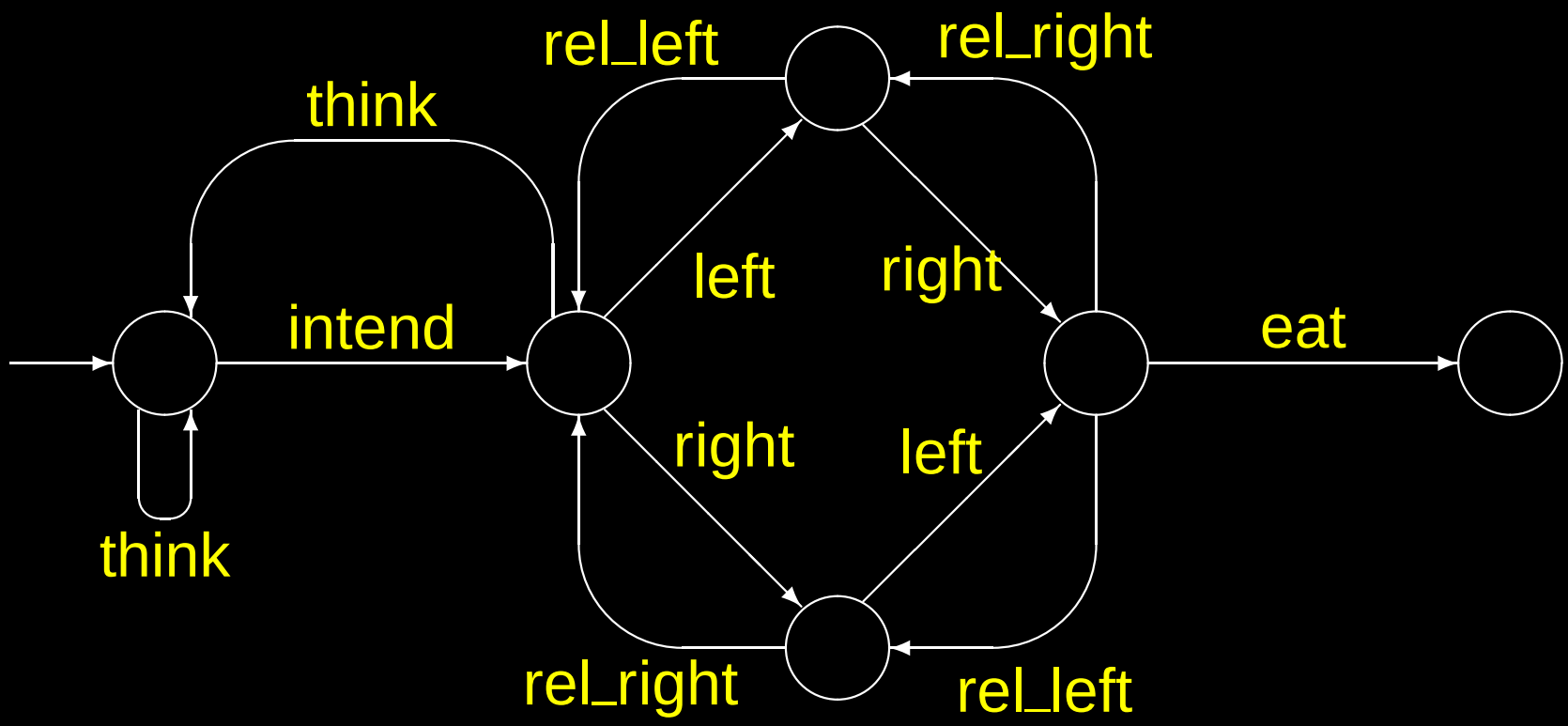
Dining Philosopher



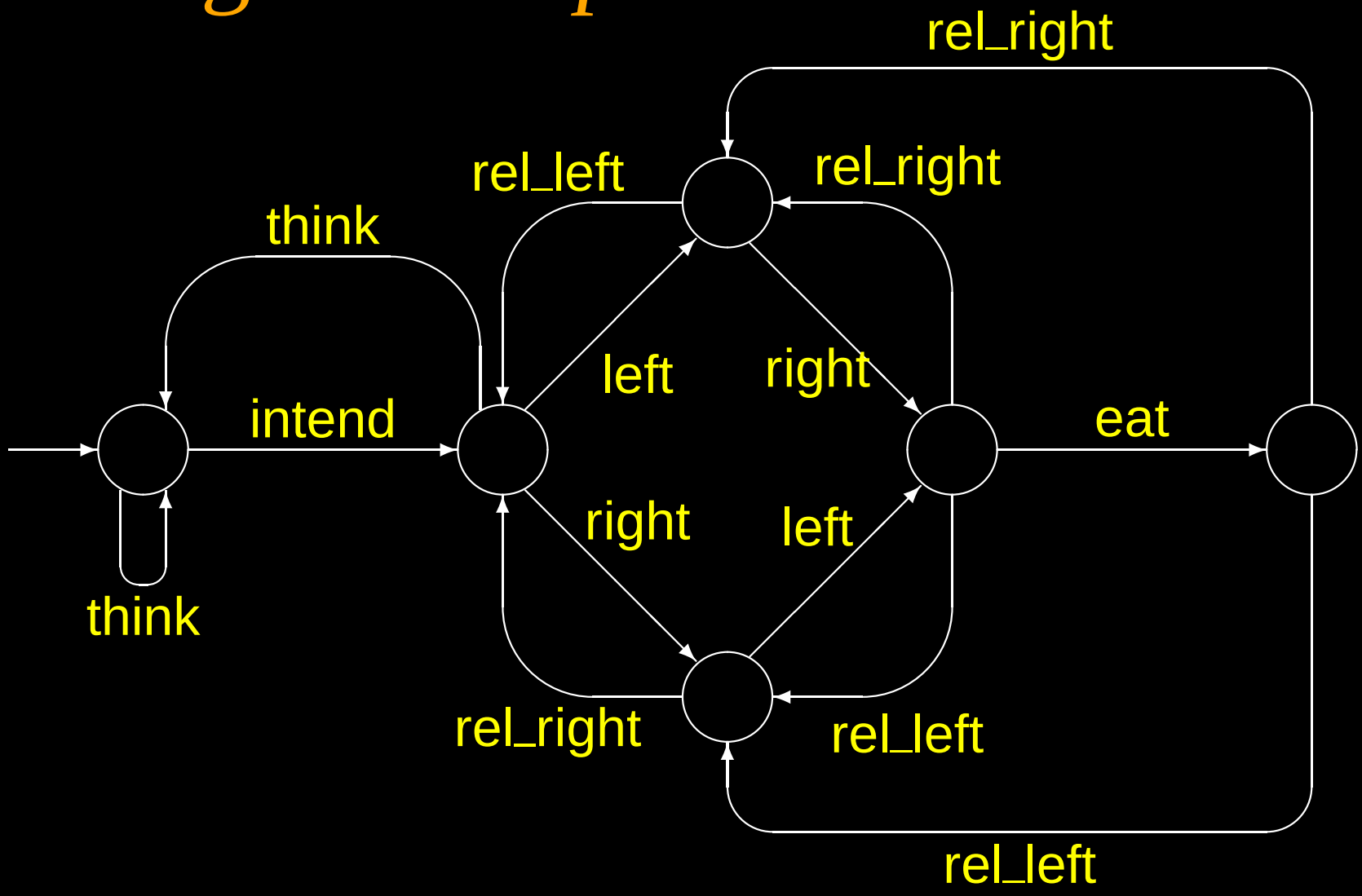
Dining Philosopher



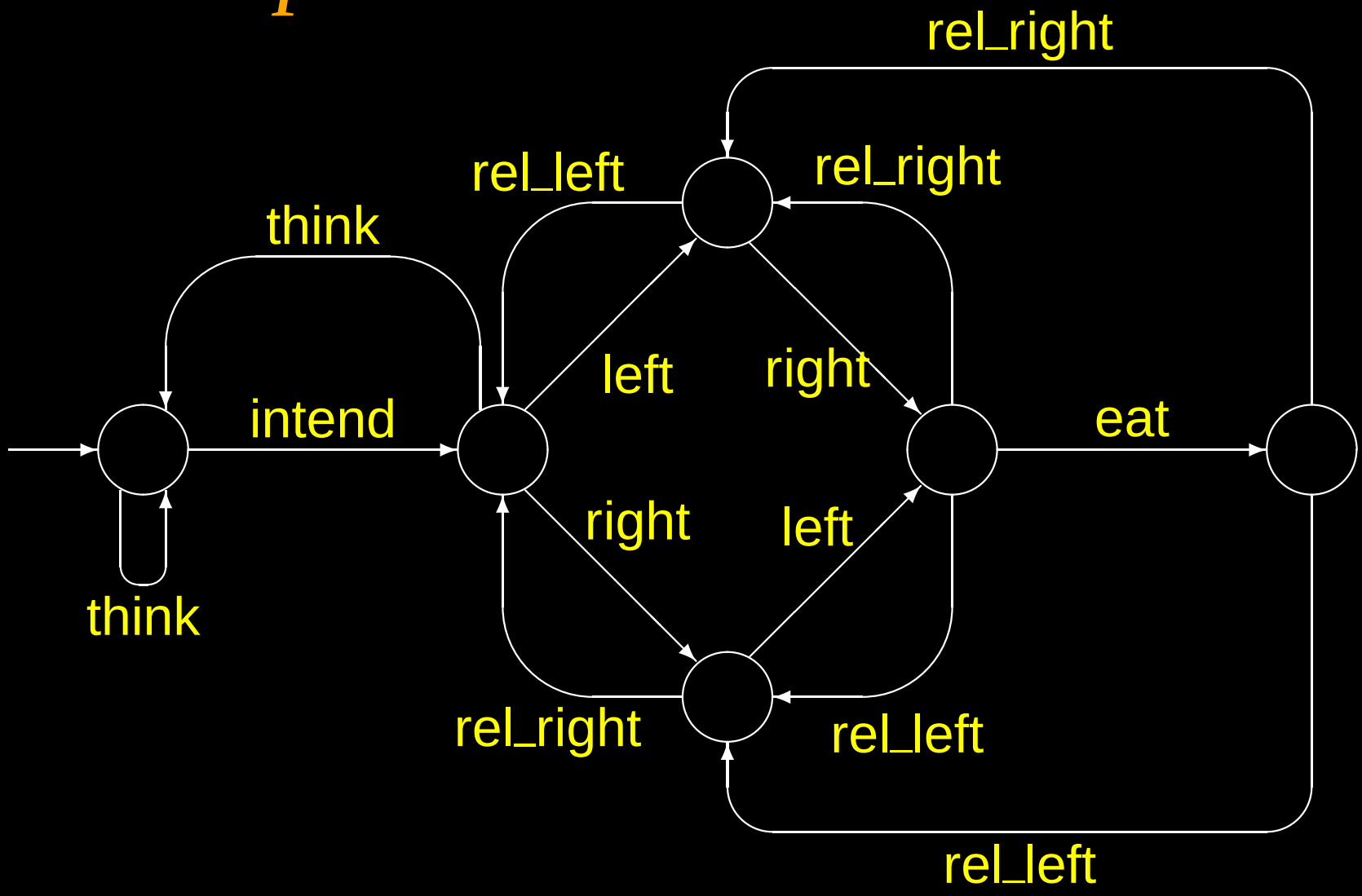
Dining Philosopher



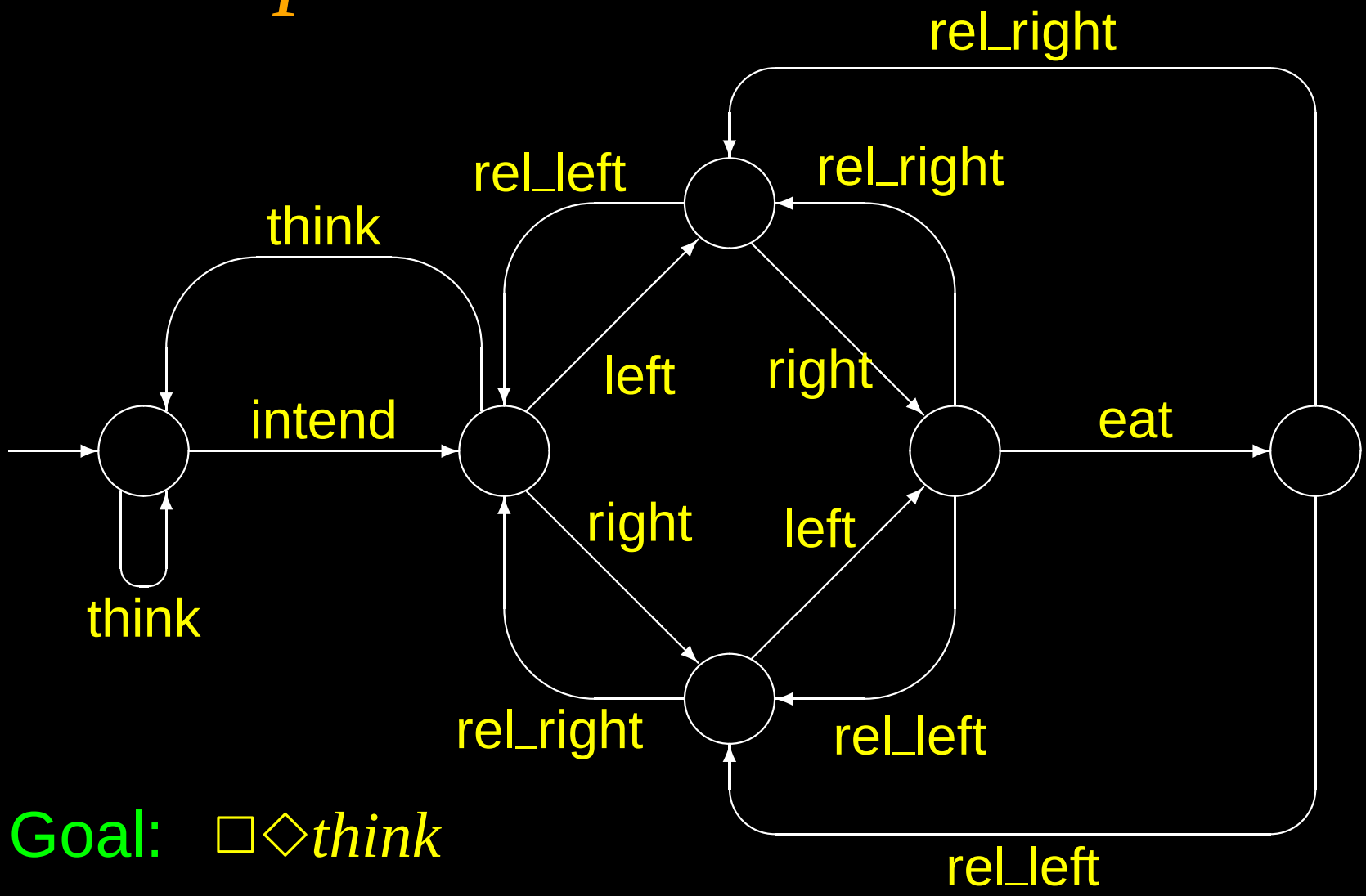
Dining Philosopher



Philosopher's Goal and Task

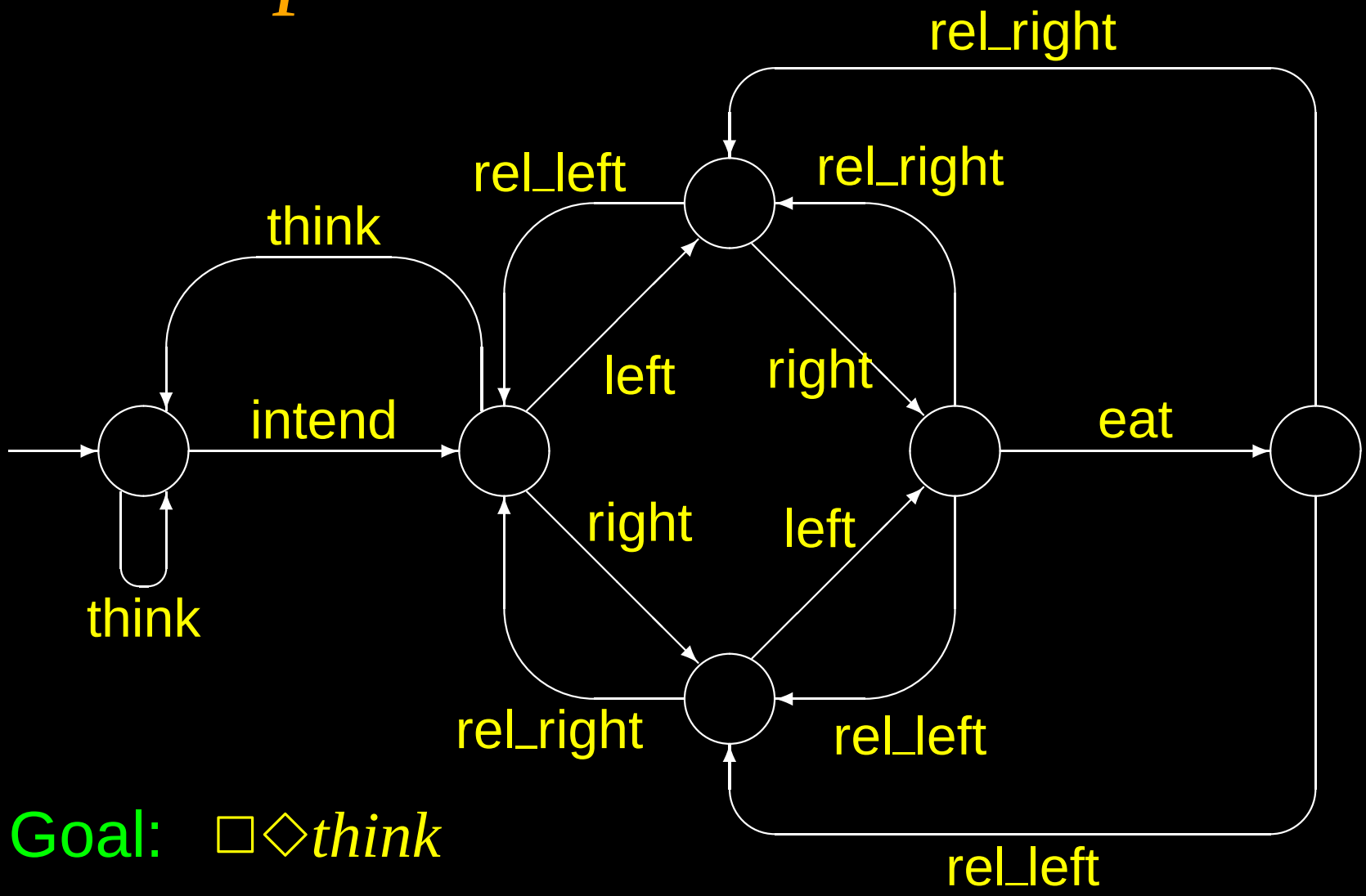


Philosopher's Goal and Task



Goal: $\Box\Diamond think$

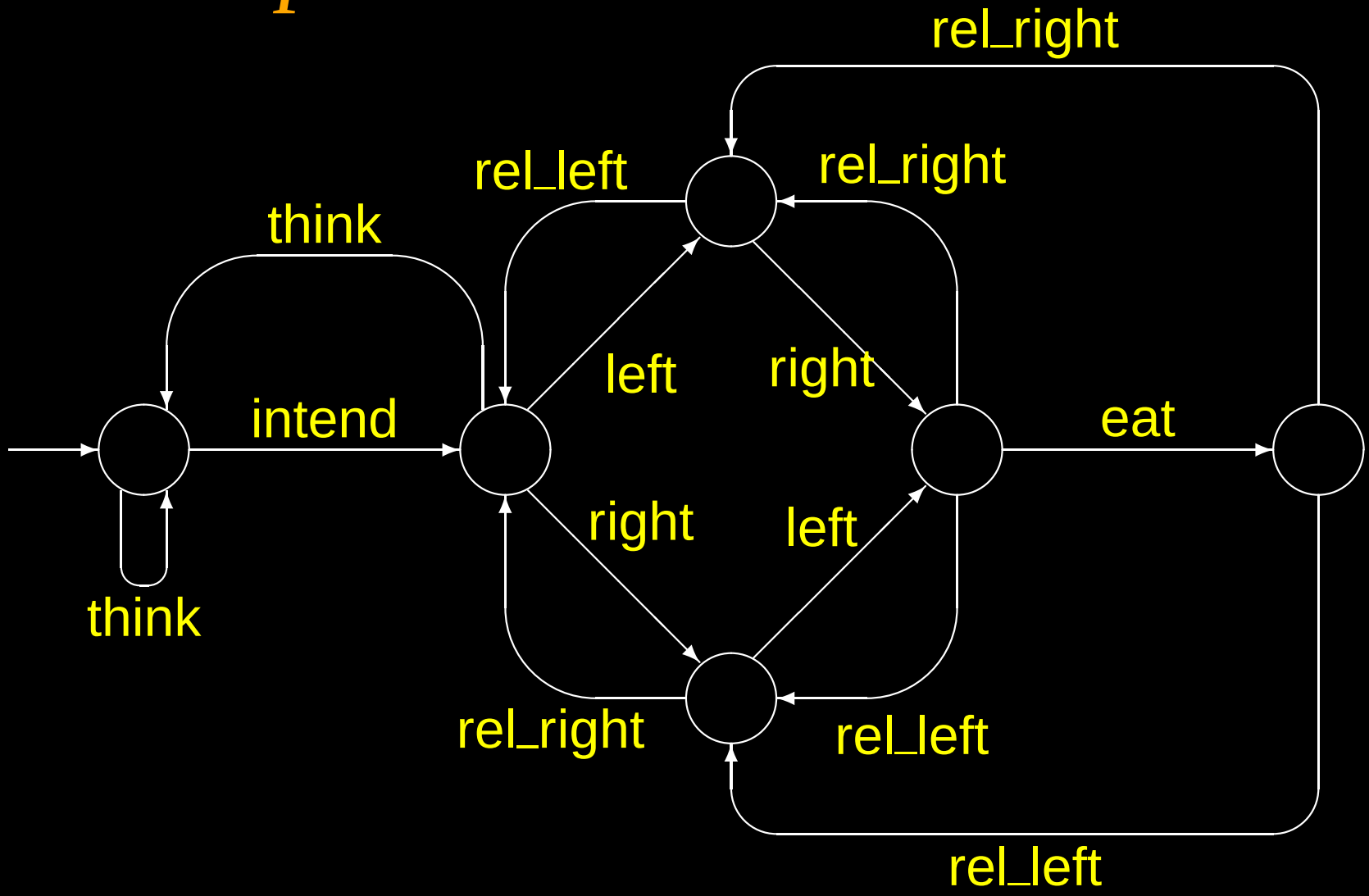
Philosopher's Goal and Task



Goal: $\Box\Diamond think$

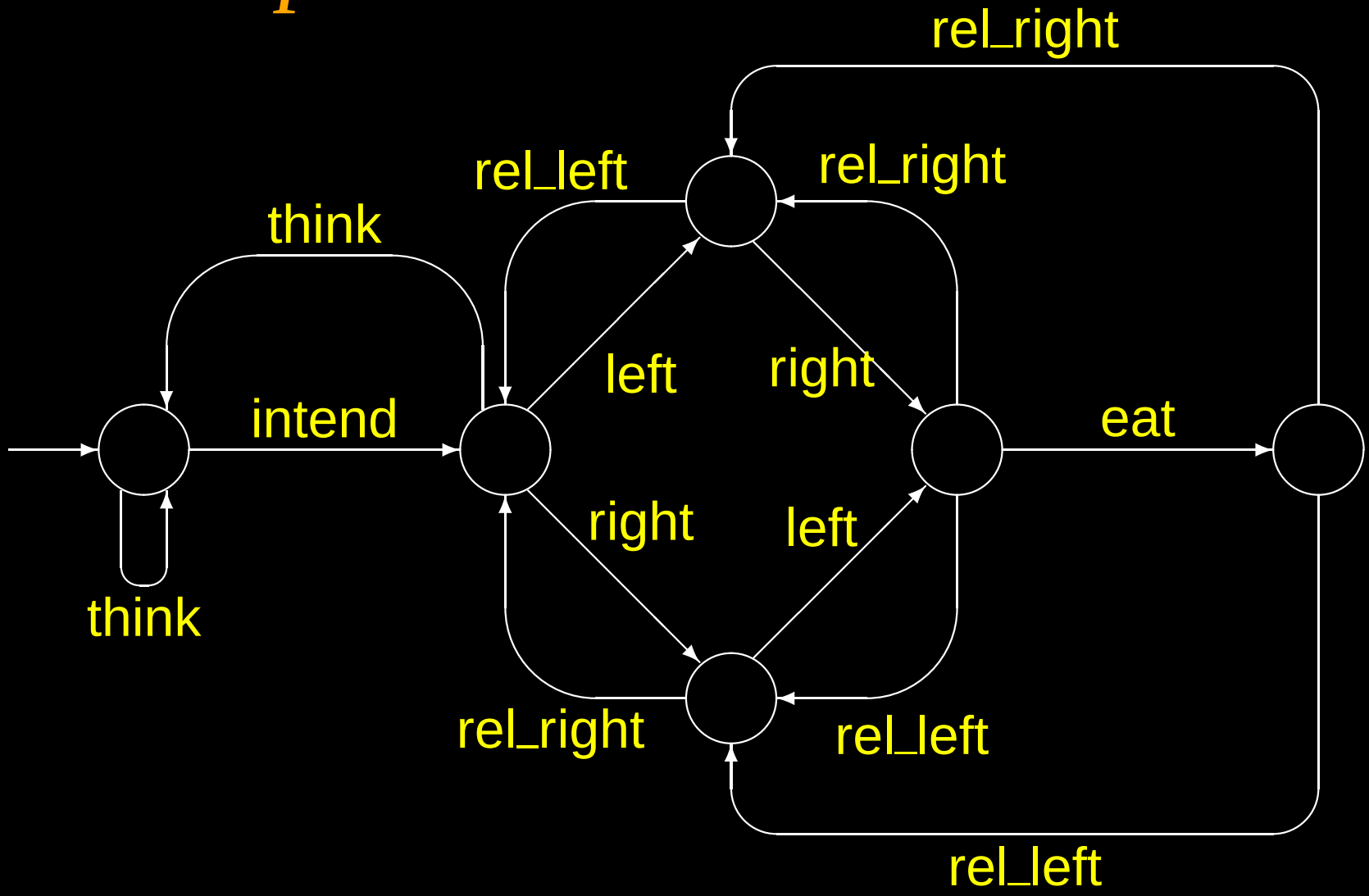
Task: $\Box((\Diamond think) \wedge (\Diamond eat))$

Philosopher's Task Failure



Task: $\Box((\Diamond think) \wedge (\Diamond eat))$

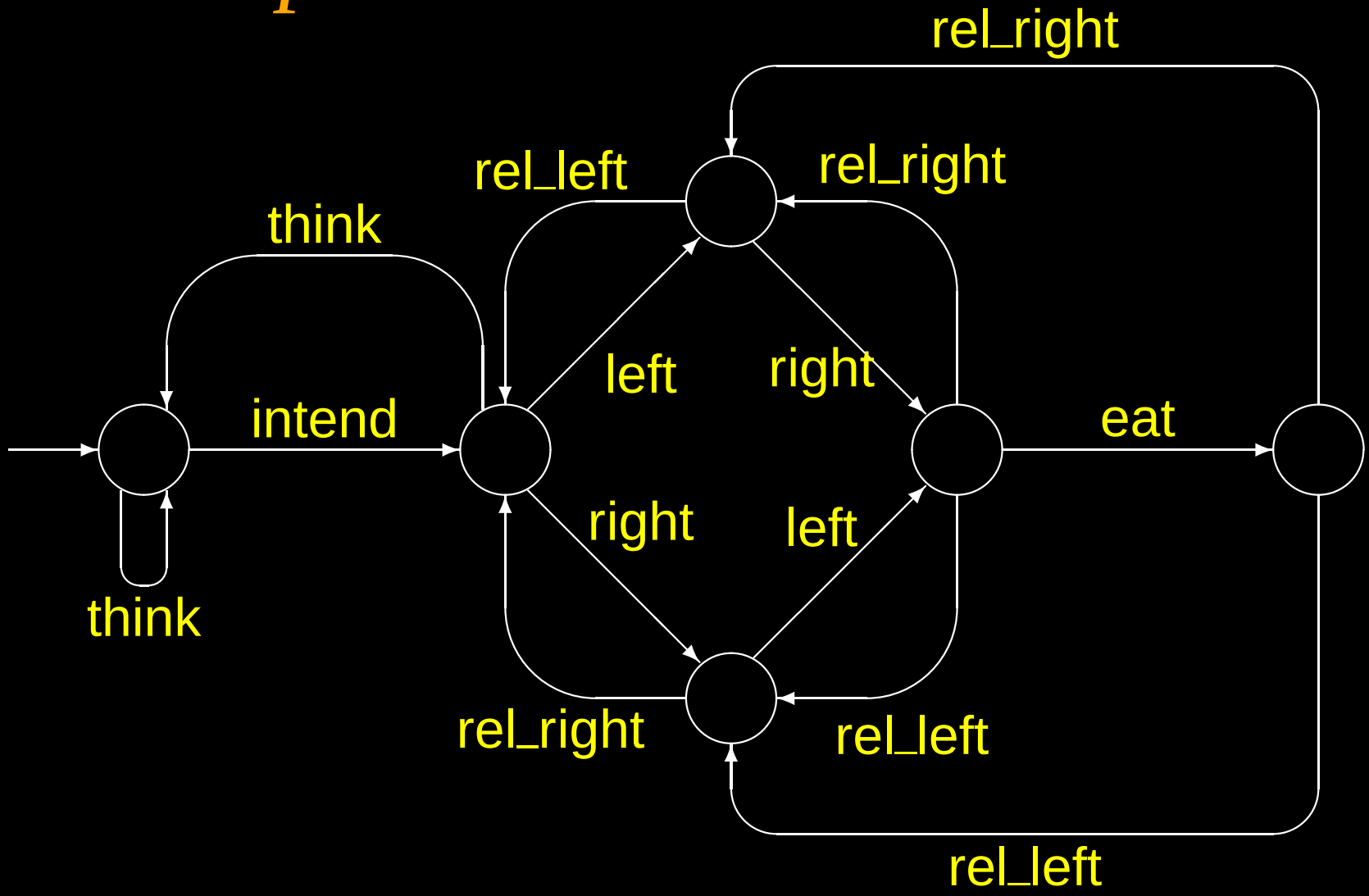
Philosopher's Task Failure



Task: $\Box((\Diamond think) \wedge (\Diamond eat))$

Task Failure: $\neg \Box((\Diamond think) \wedge (\Diamond eat))$

Philosopher's Task Failure



Task: $\Box((\Diamond think) \wedge (\Diamond eat))$

Task Failure: $\Diamond((\Box\neg think) \wedge (\Box\neg eat))$

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$

$(\Diamond think) \wedge (\Box\neg\, eat)$

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

$(\Diamond intend) \wedge \Box(\neg\, left \wedge \neg\, right)$

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

$(\Diamond intend) \wedge \Box(\neg\, left \wedge \neg\, right)$

distracted by thoughts

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

$(\Diamond intend) \wedge \Box(\neg\, left \wedge \neg\, right)$

distracted by thoughts

$(\Diamond((left \wedge \bigcirc right) \vee (right \wedge \bigcirc left))) \wedge \Box\neg\, eat$

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

$(\Diamond intend) \wedge \Box(\neg\, left \wedge \neg\, right)$

distracted by thoughts

$(\Diamond((left \wedge \bigcirc right) \vee (right \wedge \bigcirc left))) \wedge \Box\neg\, eat$

cannot use chopstics

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

$(\Diamond intend) \wedge \Box(\neg\, left \wedge \neg\, right)$

distracted by thoughts

$(\Diamond((left \wedge \bigcirc right) \vee (right \wedge \bigcirc left))) \wedge \Box\neg\, eat$

cannot use chopstics

$((\Diamond left) \vee (\Diamond right)) \wedge \Box(\neg\, left \vee \neg\, right)$

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

$(\Diamond intend) \wedge \Box(\neg\, left \wedge \neg\, right)$
distracted by thoughts

$(\Diamond((left \wedge \bigcirc right) \vee (right \wedge \bigcirc left))) \wedge \Box\neg\, eat$
cannot use chopstics

$((\Diamond left) \vee (\Diamond right)) \wedge \Box(\neg\, left \vee \neg\, right)$
unable to get two chopstics

Philosopher's Behaviour

leading to task failure $(\Box\neg\, think) \wedge (\Box\neg\, eat)$

$(\Box\neg\, think) \wedge (\Diamond eat)$ not a philosopher

$(\Diamond think) \wedge (\Box\neg\, eat)$ further decomposed

$(\Diamond intend) \wedge \Box(\neg\, left \wedge \neg\, right)$
distracted by thoughts

$(\Diamond((left \wedge \bigcirc right) \vee (right \wedge \bigcirc left))) \wedge \Box\neg\, eat$
cannot use chopstics

$((\Diamond left) \vee (\Diamond right)) \wedge \Box(\neg\, left \vee \neg\, right)$
unable to get two chopstics
further decomposed

Philosopher's Behaviour

$$((\Diamond \mathit{left}) \vee (\Diamond \mathit{right})) \wedge \Box(\neg \mathit{left} \vee \neg \mathit{right})$$

unable to get two chopstics

further decomposed

Philosopher's Behaviour

$$((\Diamond \mathit{left}) \vee (\Diamond \mathit{right})) \wedge \Box(\neg \mathit{left} \vee \neg \mathit{right})$$

unable to get two chopstics

further decomposed

$$(\Diamond \mathit{left}) \wedge \Box \neg \mathit{right}$$

Philosopher's Behaviour

$$((\Diamond left) \vee (\Diamond right)) \wedge \Box(\neg\, left \vee \neg\, right)$$

unable to get two chopstics

further decomposed

$$(\Diamond left) \wedge \Box \neg\, right$$

physical problem

Philosopher's Behaviour

$$((\Diamond left) \vee (\Diamond right)) \wedge \Box(\neg\, left \vee \neg\, right)$$

unable to get two chopstics

further decomposed

$$(\Diamond left) \wedge \Box\neg\, right$$

physical problem

$$(\Diamond right) \wedge \Box\neg\, left$$

physical problem

Philosopher's Behaviour

$$((\Diamond left) \vee (\Diamond right)) \wedge \Box(\neg left \vee \neg right)$$

unable to get two chopstics

further decomposed

$$(\Diamond left) \wedge \Box \neg right$$

physical problem

$$(\Diamond right) \wedge \Box \neg left$$

physical problem

$$(\Diamond left) \wedge (\Diamond right) \wedge \Box(\neg left \vee \neg right)$$

Philosopher's Behaviour

$((\Diamond left) \vee (\Diamond right)) \wedge \Box(\neg left \vee \neg right)$

unable to get two chopstics

further decomposed

$(\Diamond left) \wedge \Box \neg right$

physical problem

$(\Diamond right) \wedge \Box \neg left$

physical problem

$(\Diamond left) \wedge (\Diamond right) \wedge \Box(\neg left \vee \neg right)$

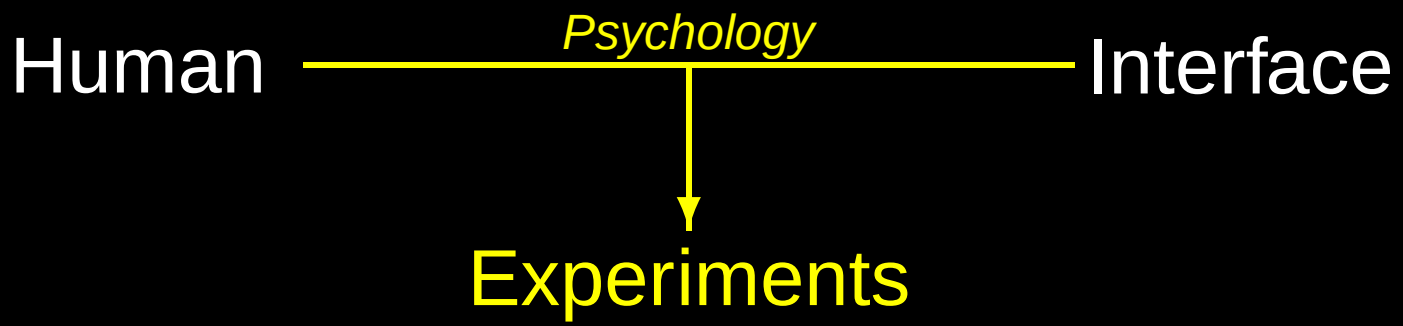
does not understand

Big Picture

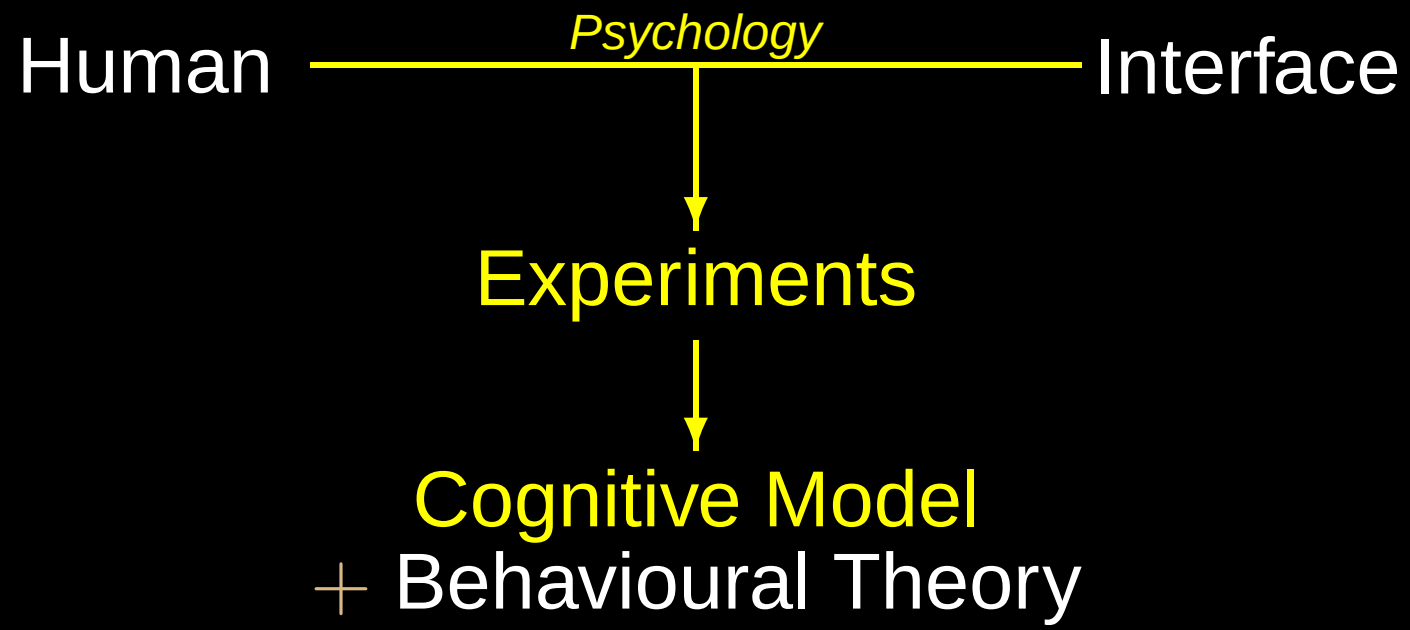
Human

Interface

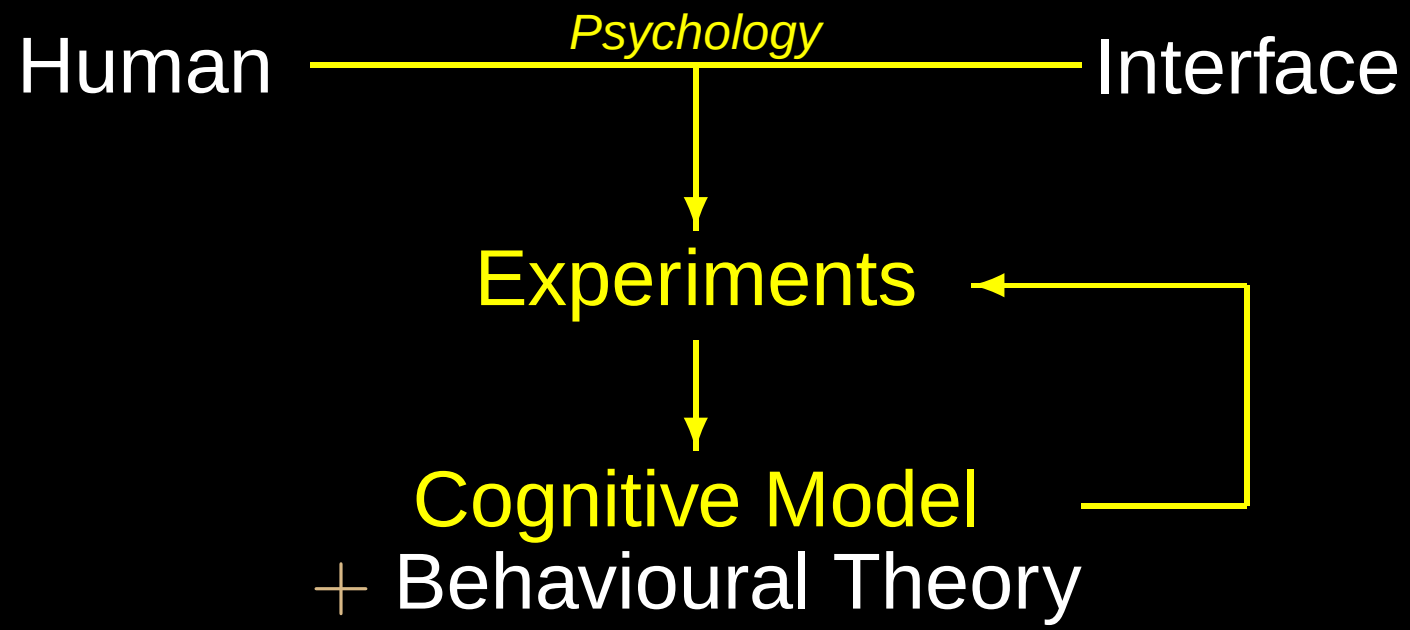
Big Picture



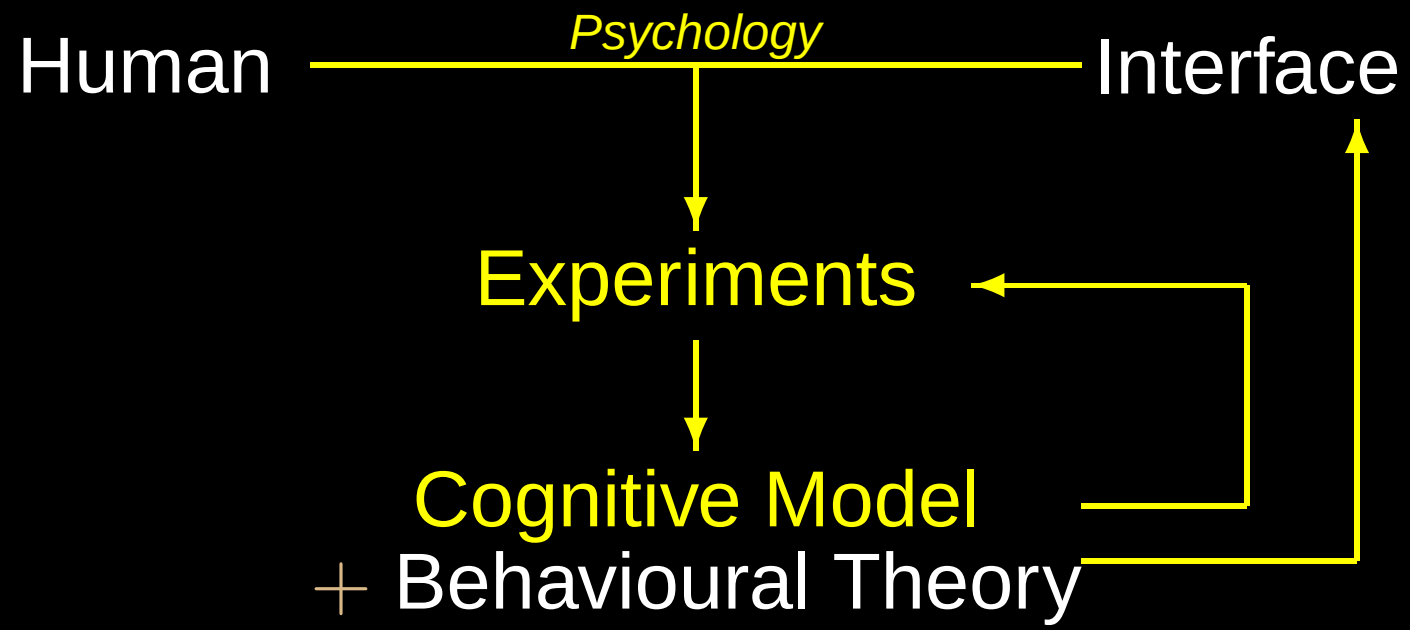
Big Picture


Human
Psychology
Interface
Experiments
Cognitive Model
+ Behavioural Theory

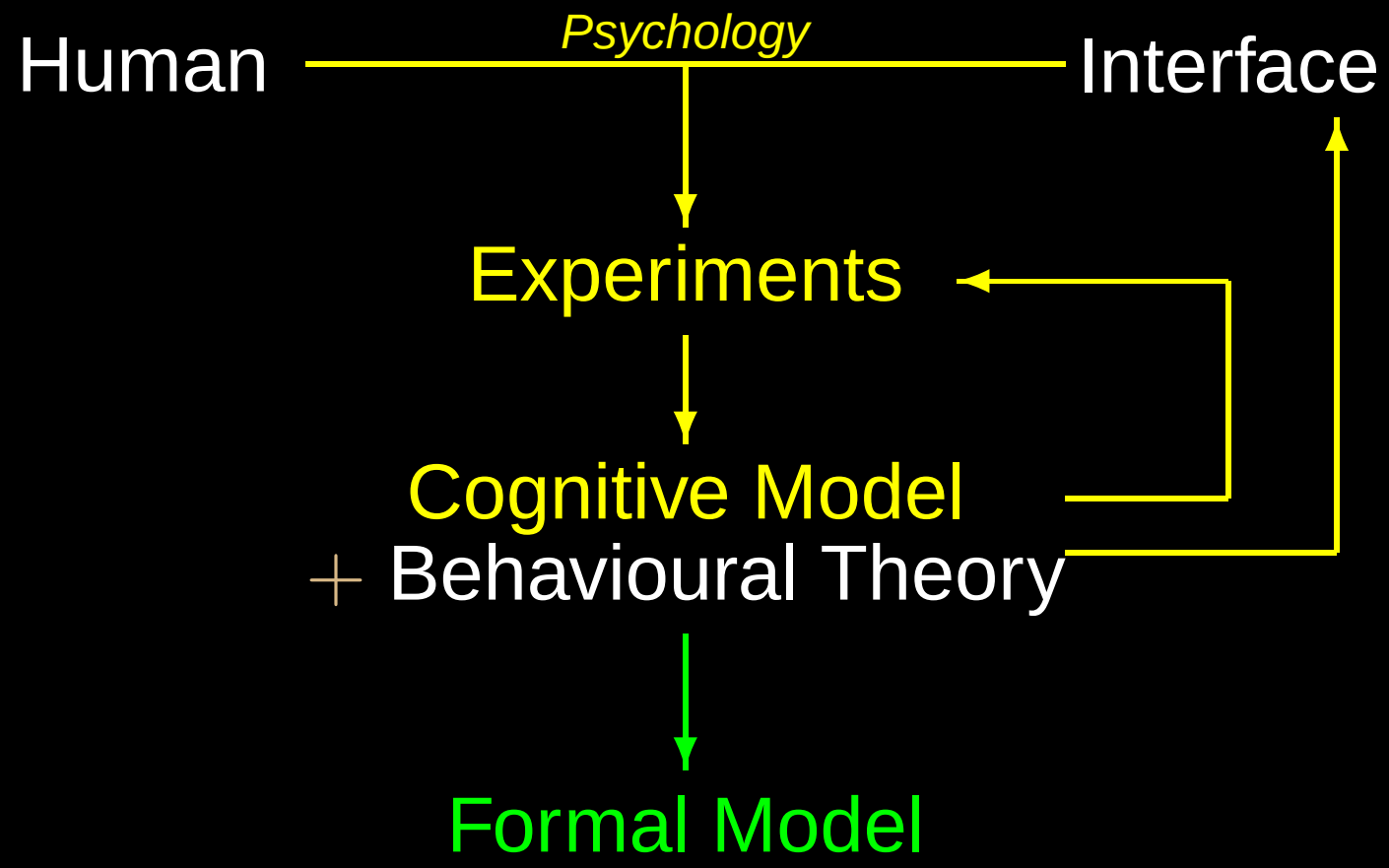
Big Picture


Human
Psychology
Interface
Experiments
Cognitive Model
+ Behavioural Theory

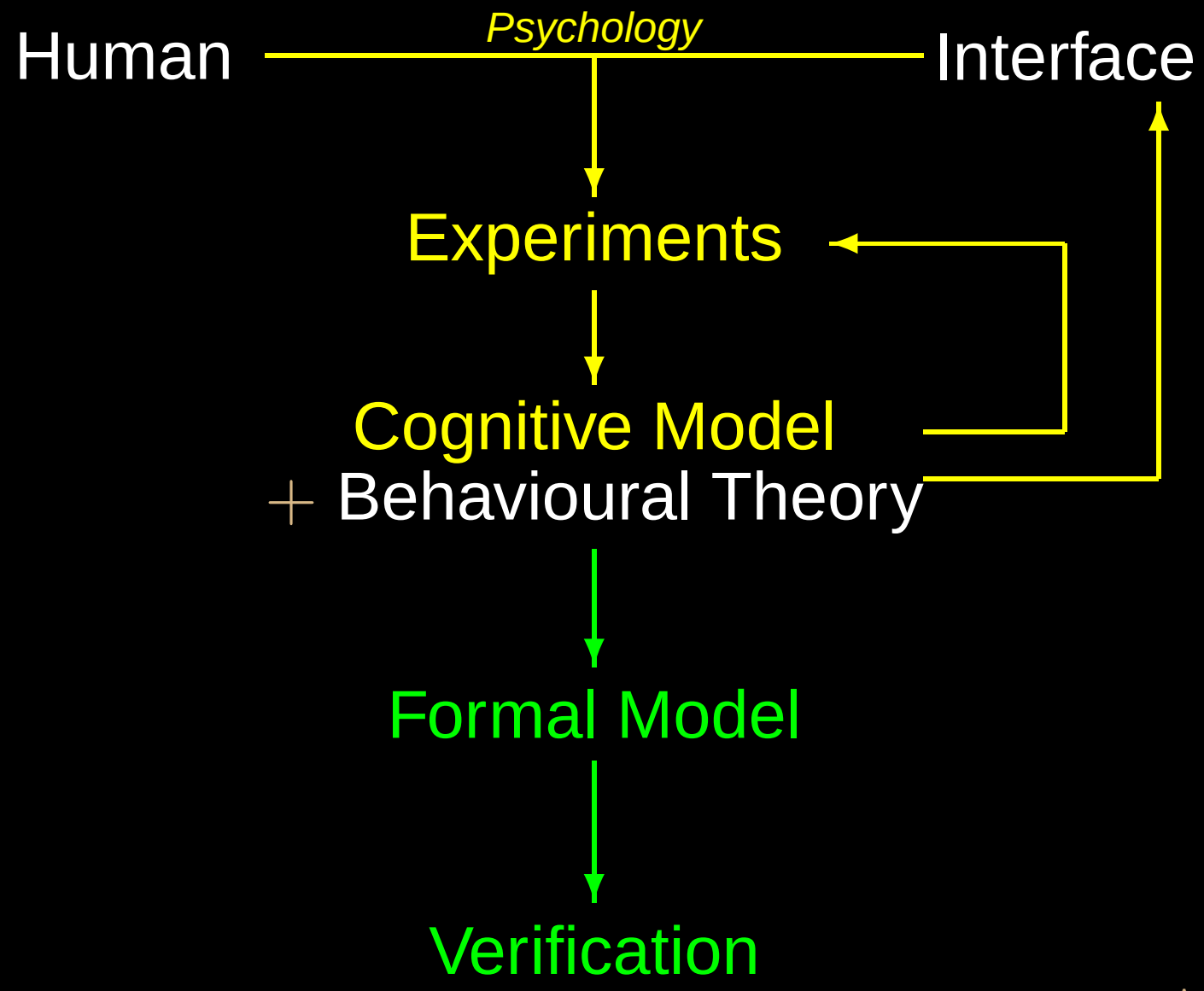
Big Picture


Human
Psychology
Interface
Experiments
Cognitive Model
+ Behavioural Theory

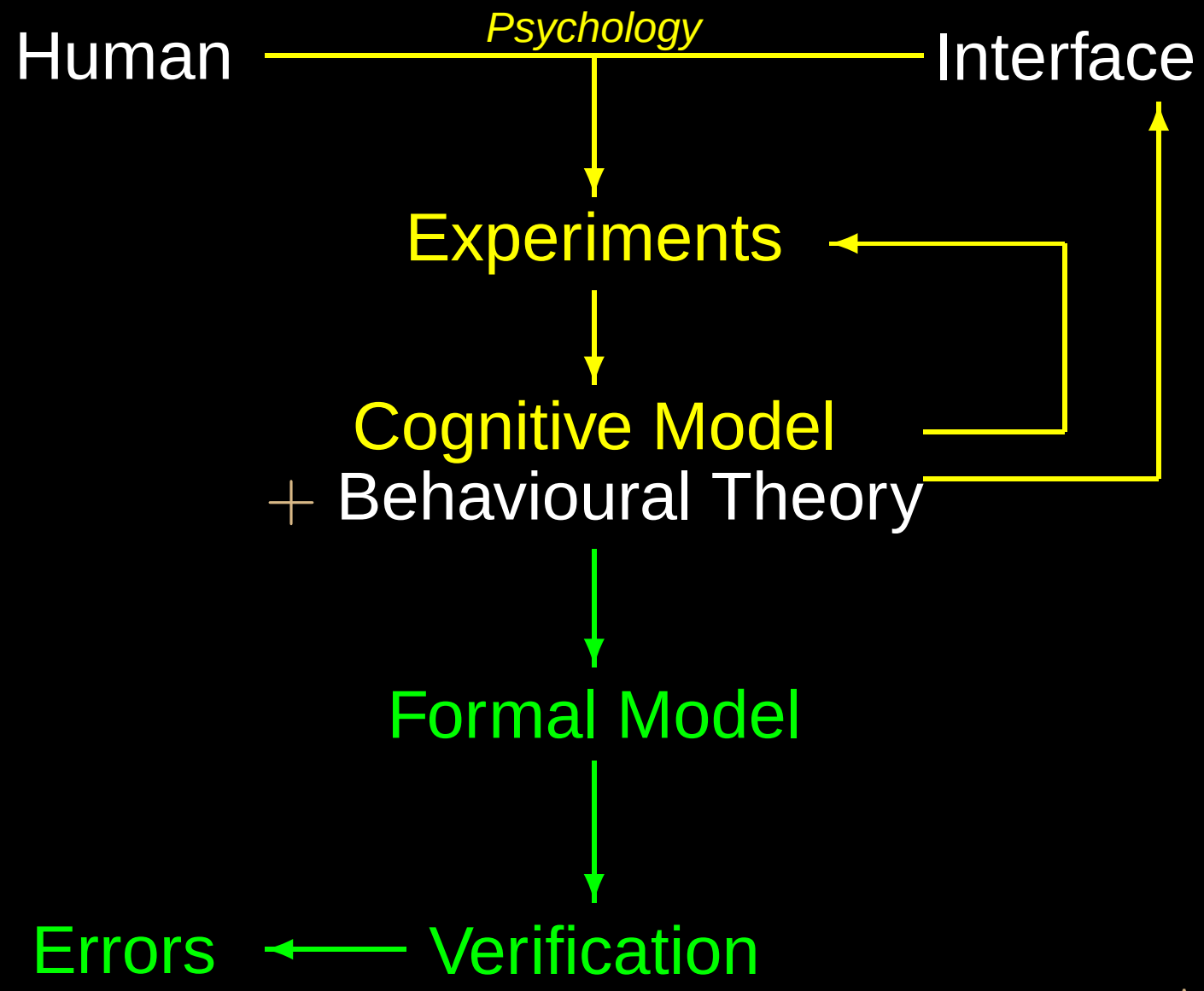
Big Picture


Human
Psychology
Interface
Experiments
Cognitive Model
+ Behavioural Theory
Formal Model

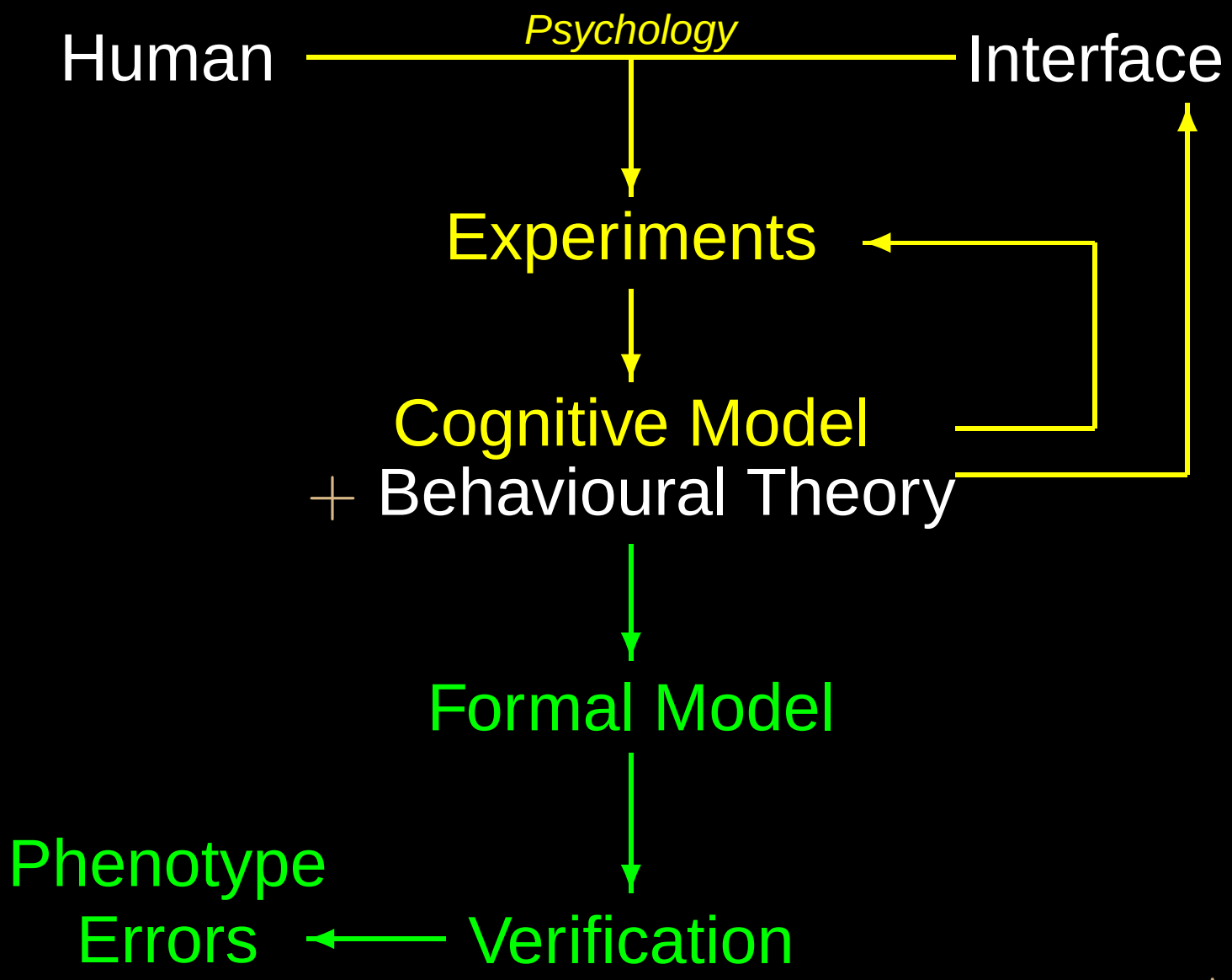
Big Picture


Human
Psychology
Interface
Experiments
Cognitive Model
+ Behavioural Theory
Formal Model
Verification

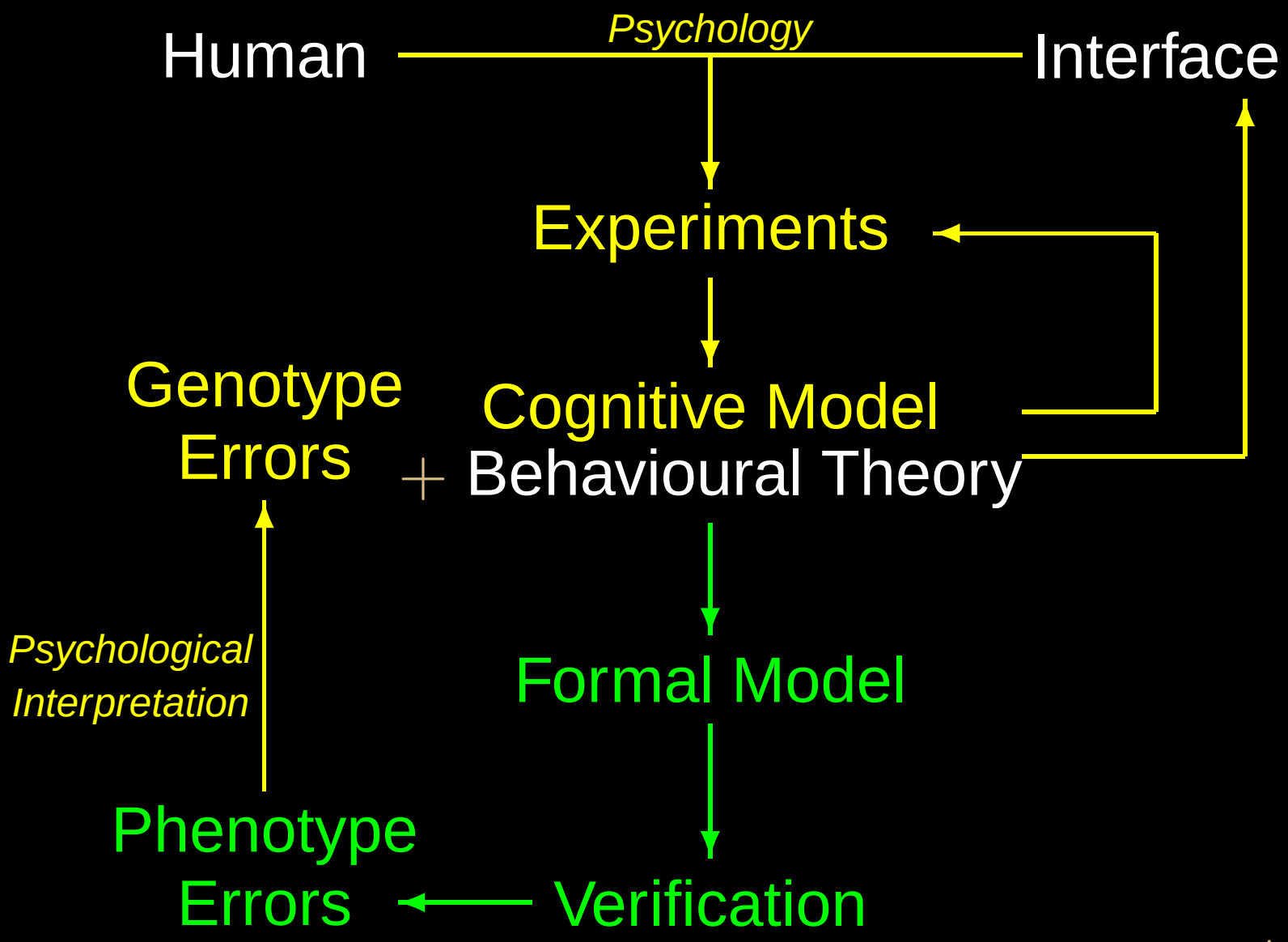
Big Picture


Human
Psychology
Interface
Experiments
Cognitive Model
+ Behavioural Theory
Formal Model
Errors
Verification

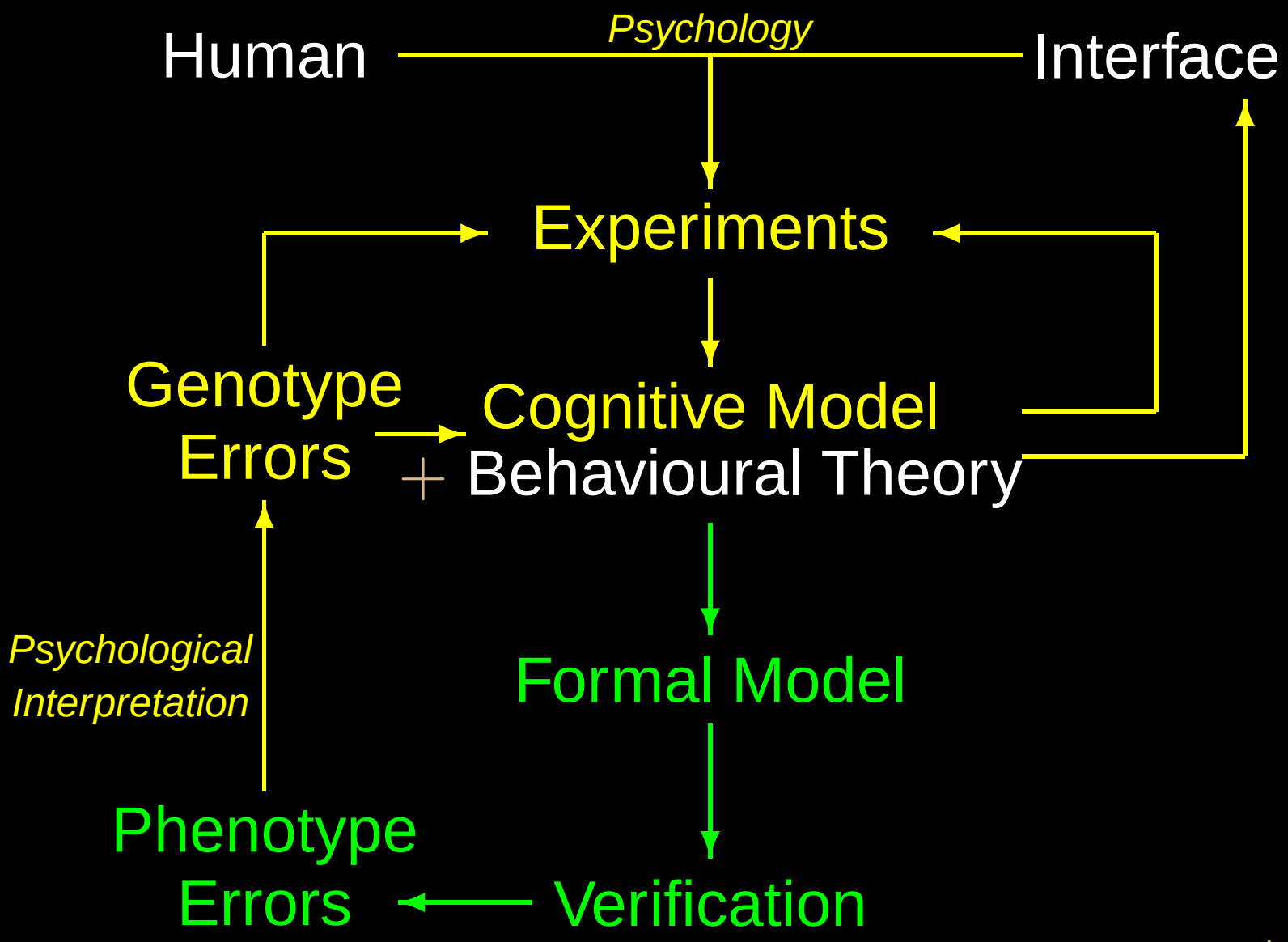
Big Picture


Human
Psychology
Interface
Experiments
Cognitive Model
+ Behavioural Theory
Formal Model
Phenotype
Errors
Verification

Big Picture


Human
Psychology
Interface
Experiments
Genotype
Errors
Cognitive Model
+ Behavioural Theory
Psychological
Interpretation
Formal Model
Phenotype
Errors
Verification

Big Picture


Human
Psychology
Interface
Experiments
Genotype
Errors
Cognitive Model
+ Behavioural Theory
Psychological
Interpretation
Formal Model
Phenotype
Errors
Verification

History of Model-checking

- 1980s: Model-checking

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification
  - State Explosion Problem

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification
  - State Explosion Problem
- 1990s:

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification
  - State Explosion Problem
- 1990s:
  - Symbolic Model-checking *[MacMillan]*

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification
  - State Explosion Problem
- 1990s:
  - Symbolic Model-checking *[MacMillan]*
  - Abstraction

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification
  - State Explosion Problem
- 1990s:
  - Symbolic Model-checking *[MacMillan]*
  - Abstraction
  - State Explosion Contained

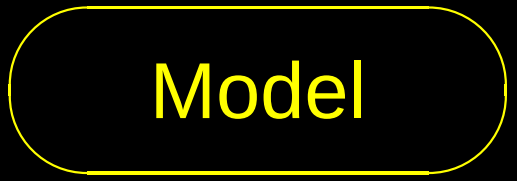
History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification
  - State Explosion Problem
- 1990s:
  - Symbolic Model-checking *[MacMillan]*
  - Abstraction
  - State Explosion Contained
  - Infinite Model-checking

History of Model-checking

- 1980s: Model-checking
  - *[Emerson and Clarke]*
  - Hardware Verification
  - State Explosion Problem
- 1990s:
  - Symbolic Model-checking *[MacMillan]*
  - Abstraction
  - State Explosion Contained
  - Infinite Model-checking
  - Software Verification

Model-checking

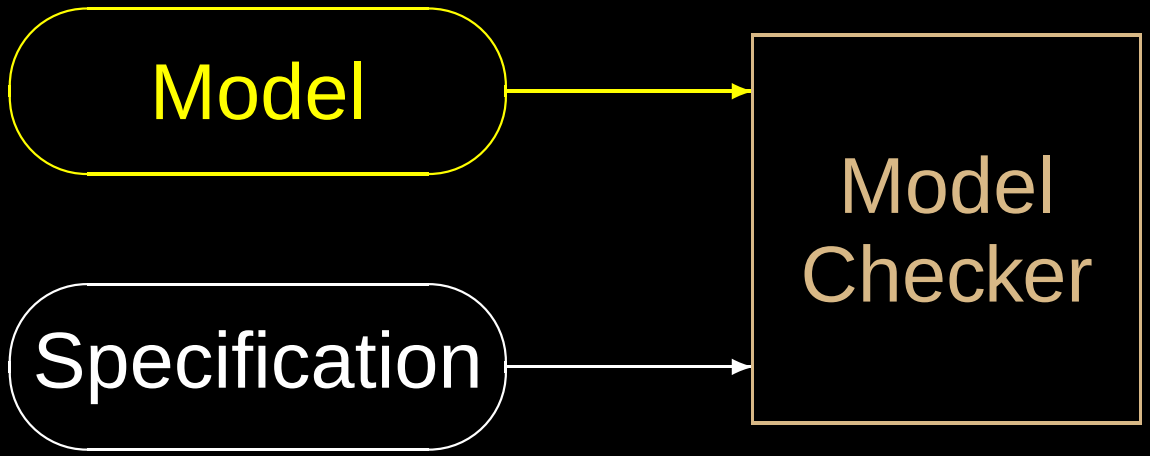


Model-checking

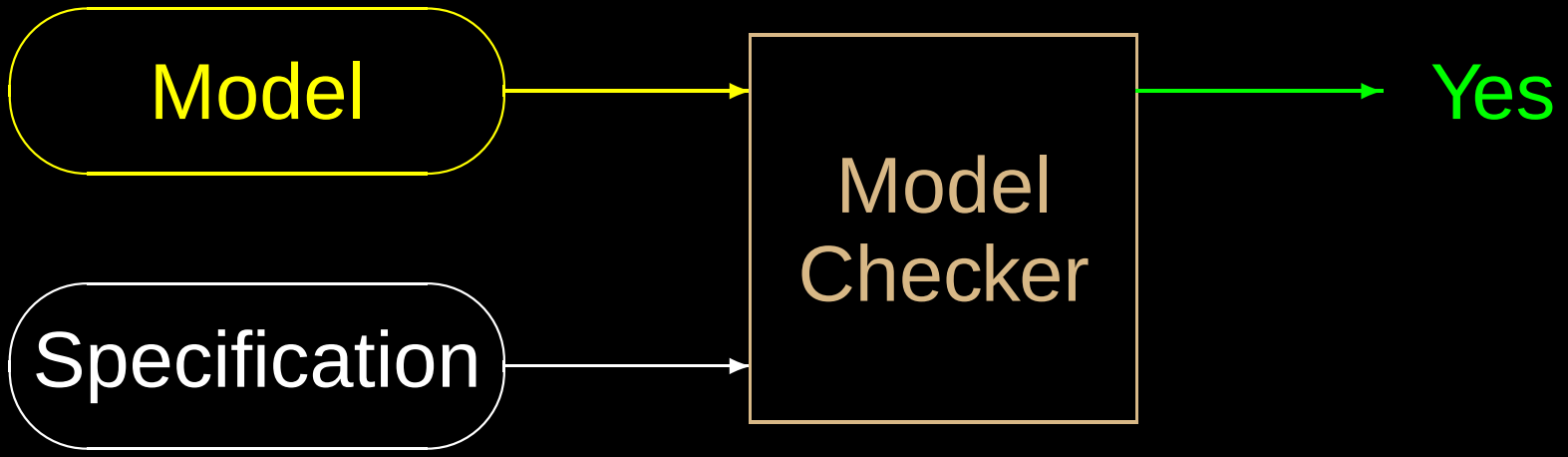
Model

Specification

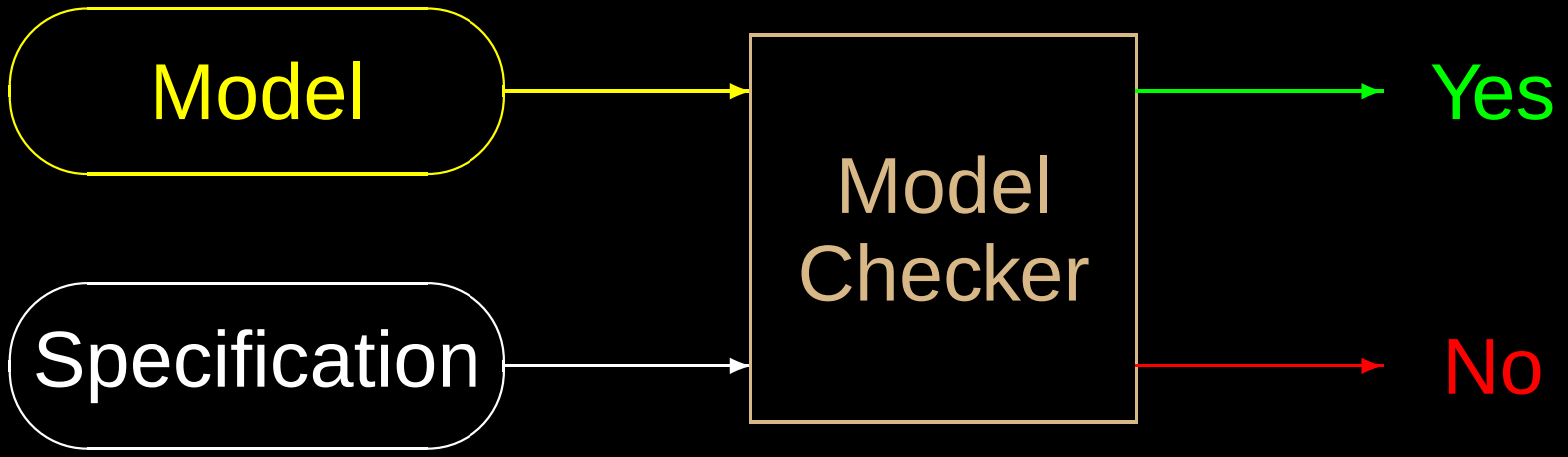
Model-checking



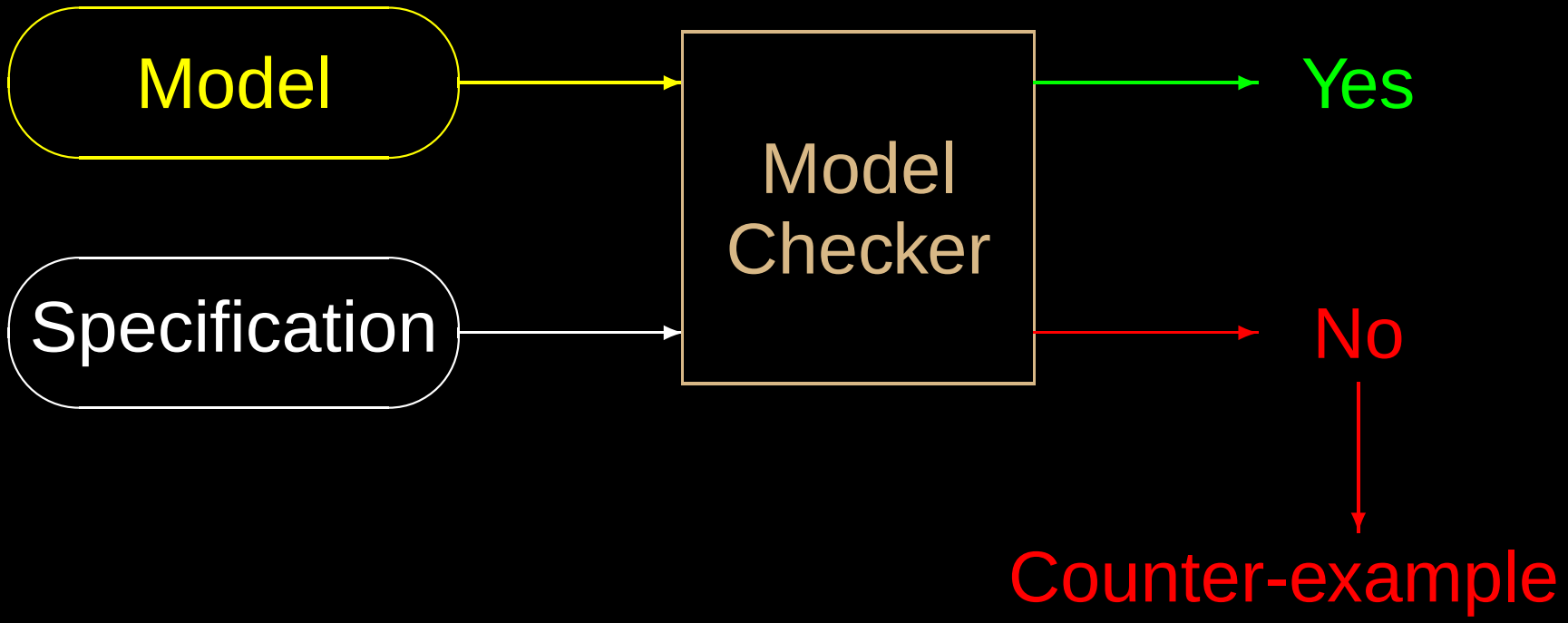
Model-checking



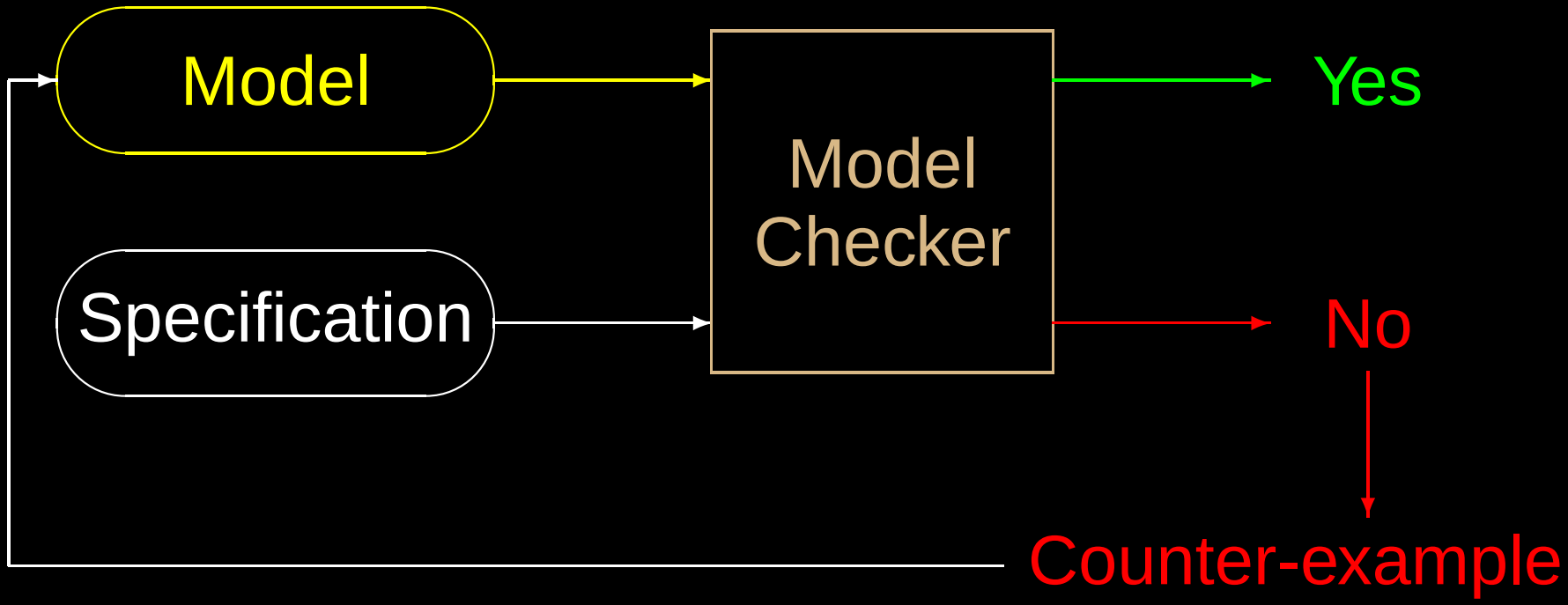
Model-checking



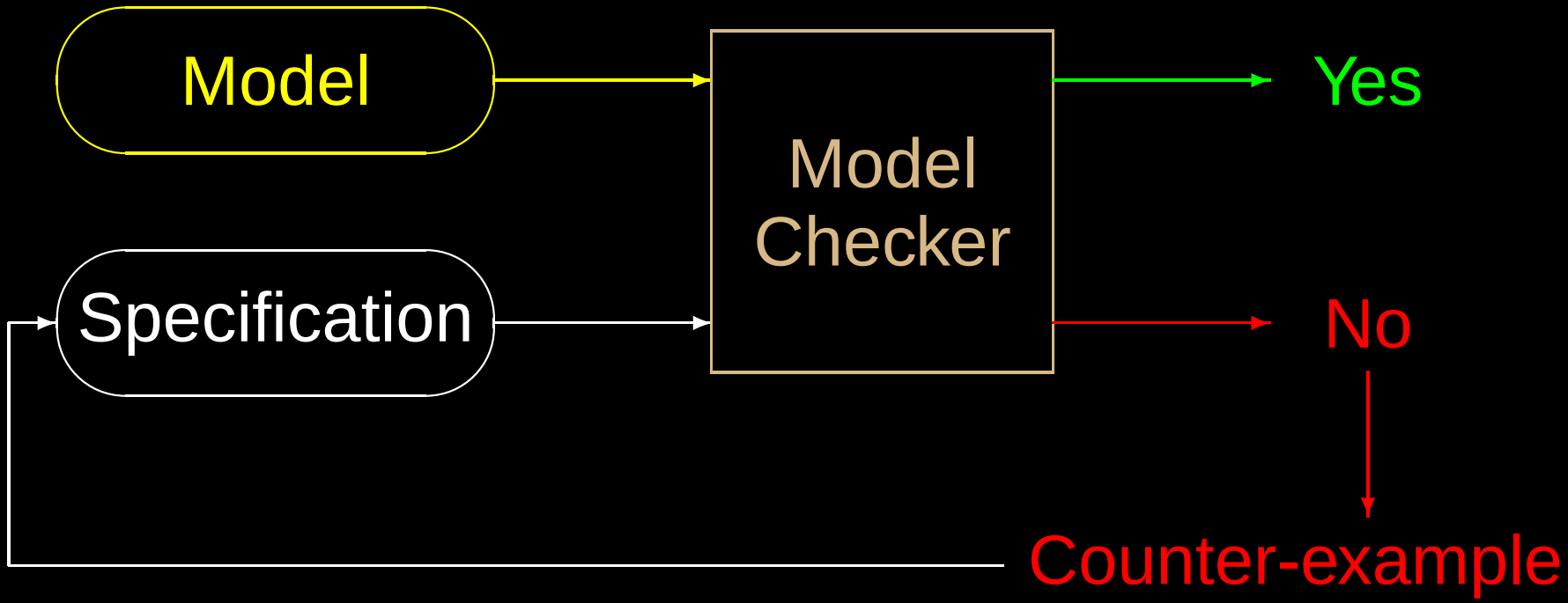
Model-checking



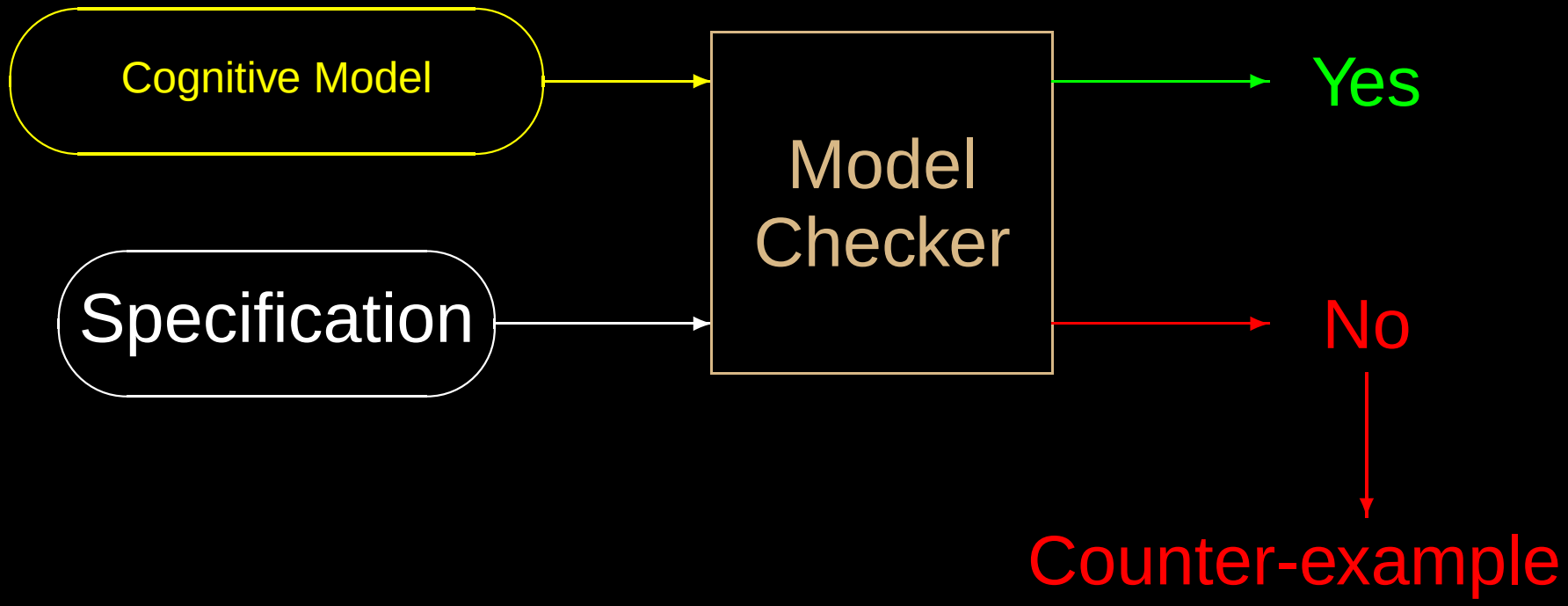
Model-checking



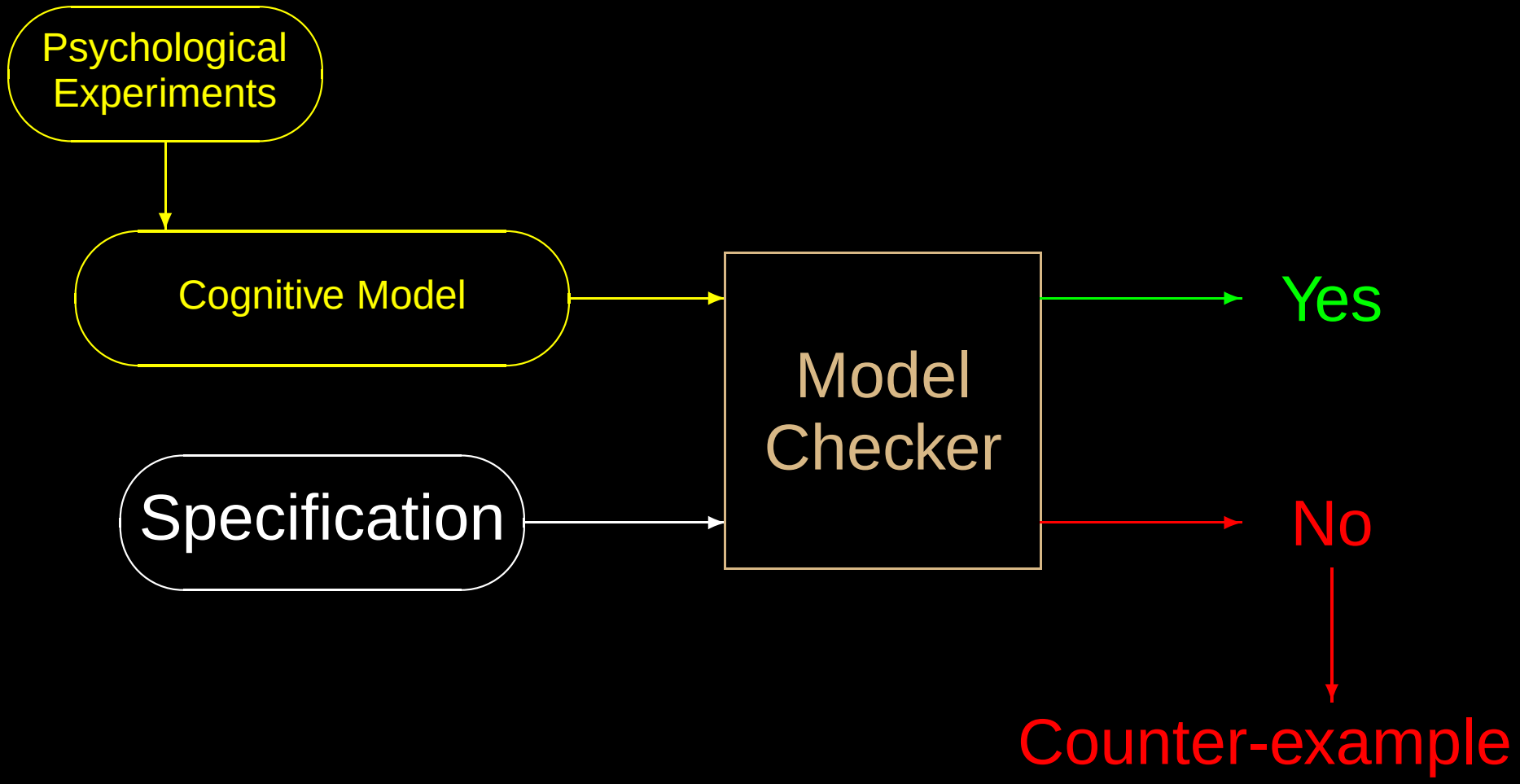
Model-checking



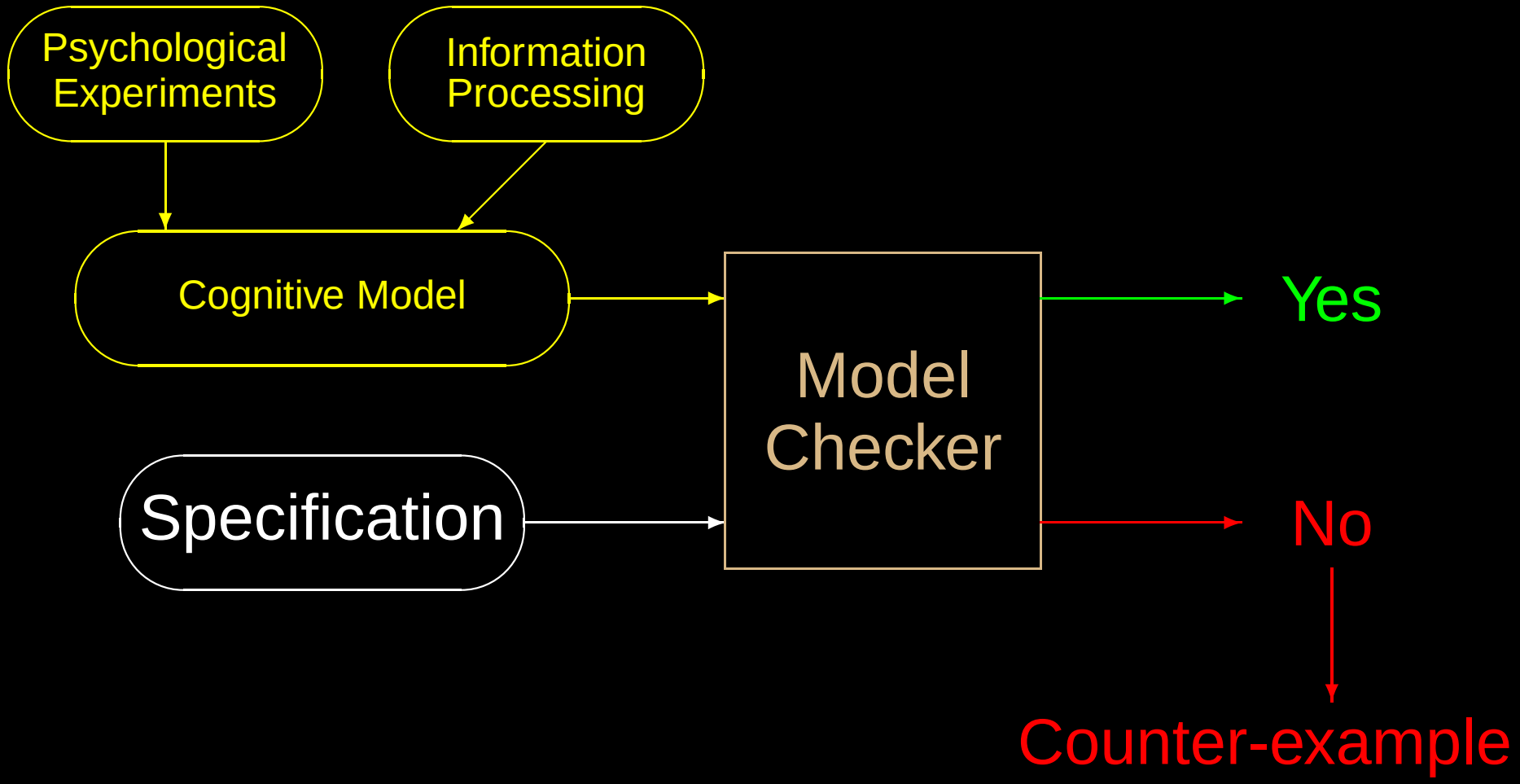
MC and Cognitive Psychology



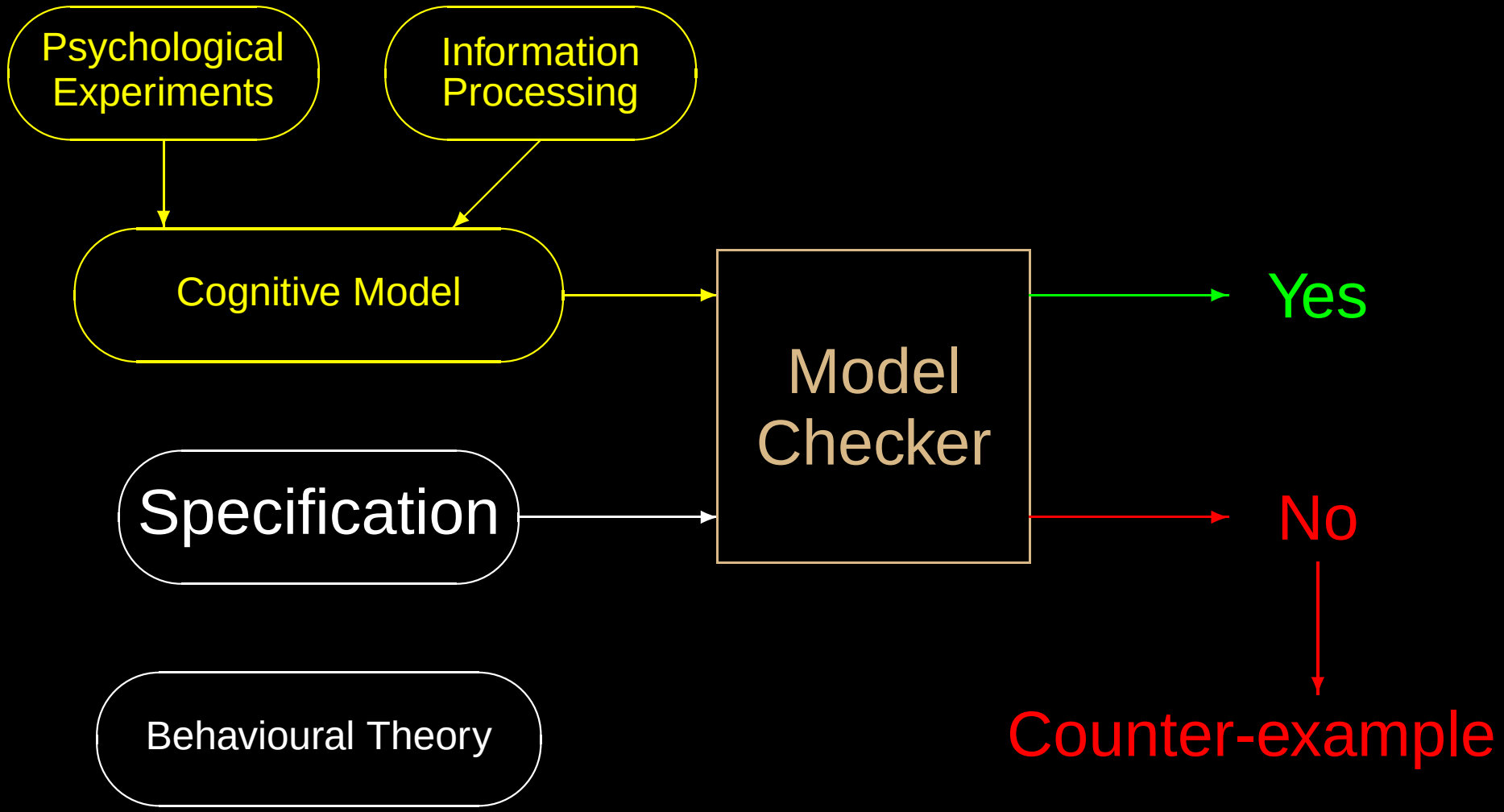
MC and Cognitive Psychology



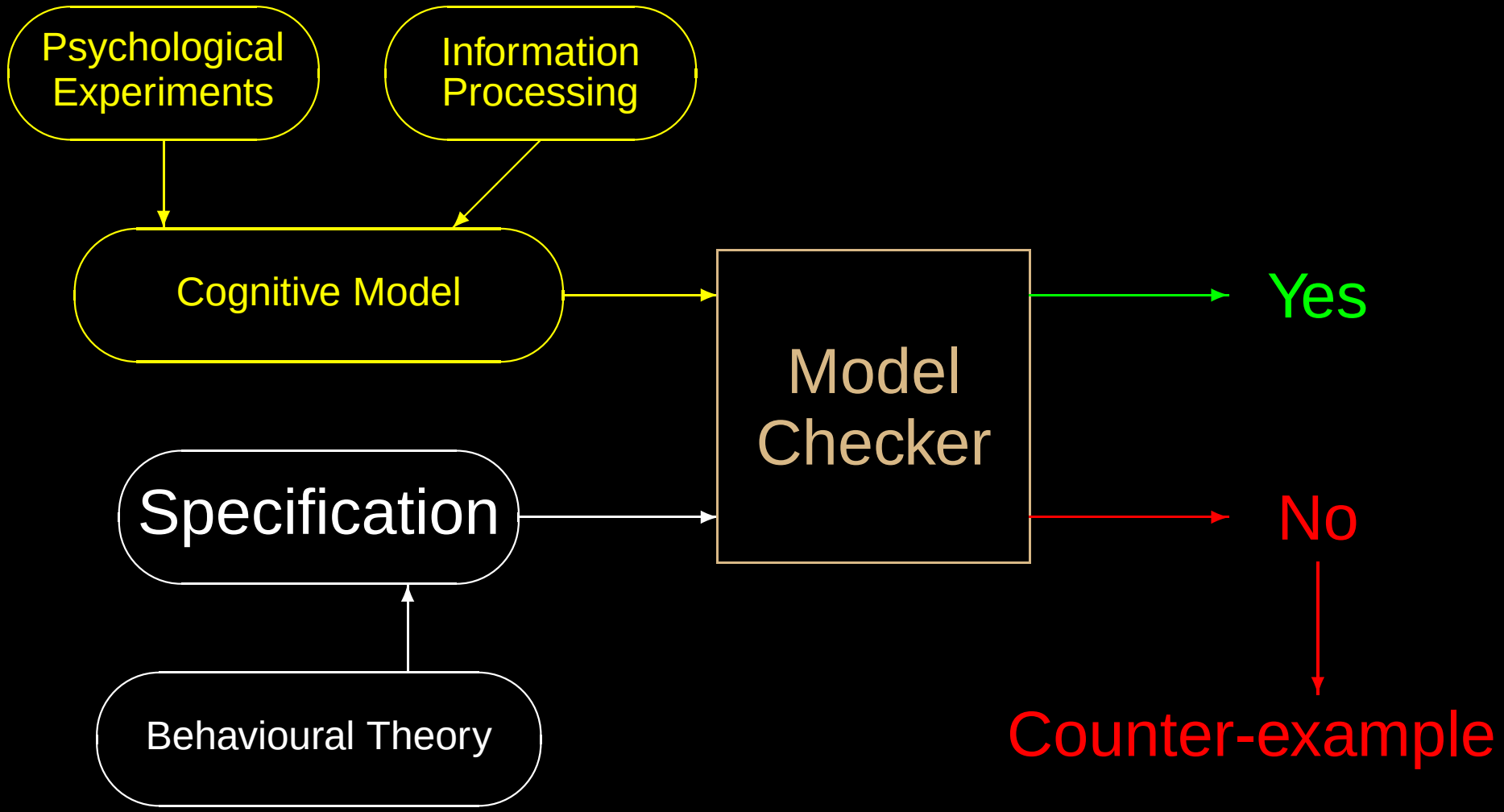
MC and Cognitive Psychology



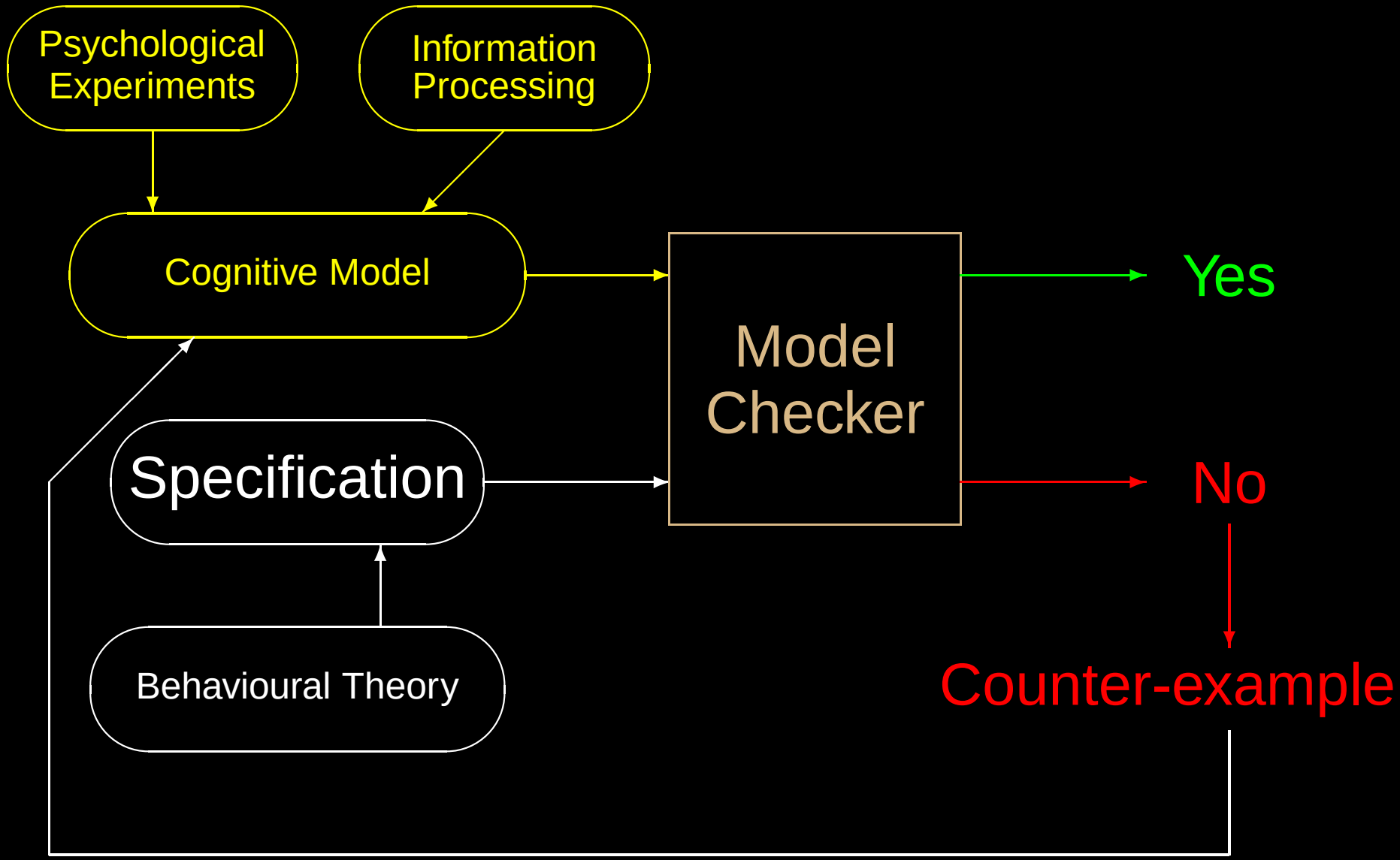
MC and Cognitive Psychology



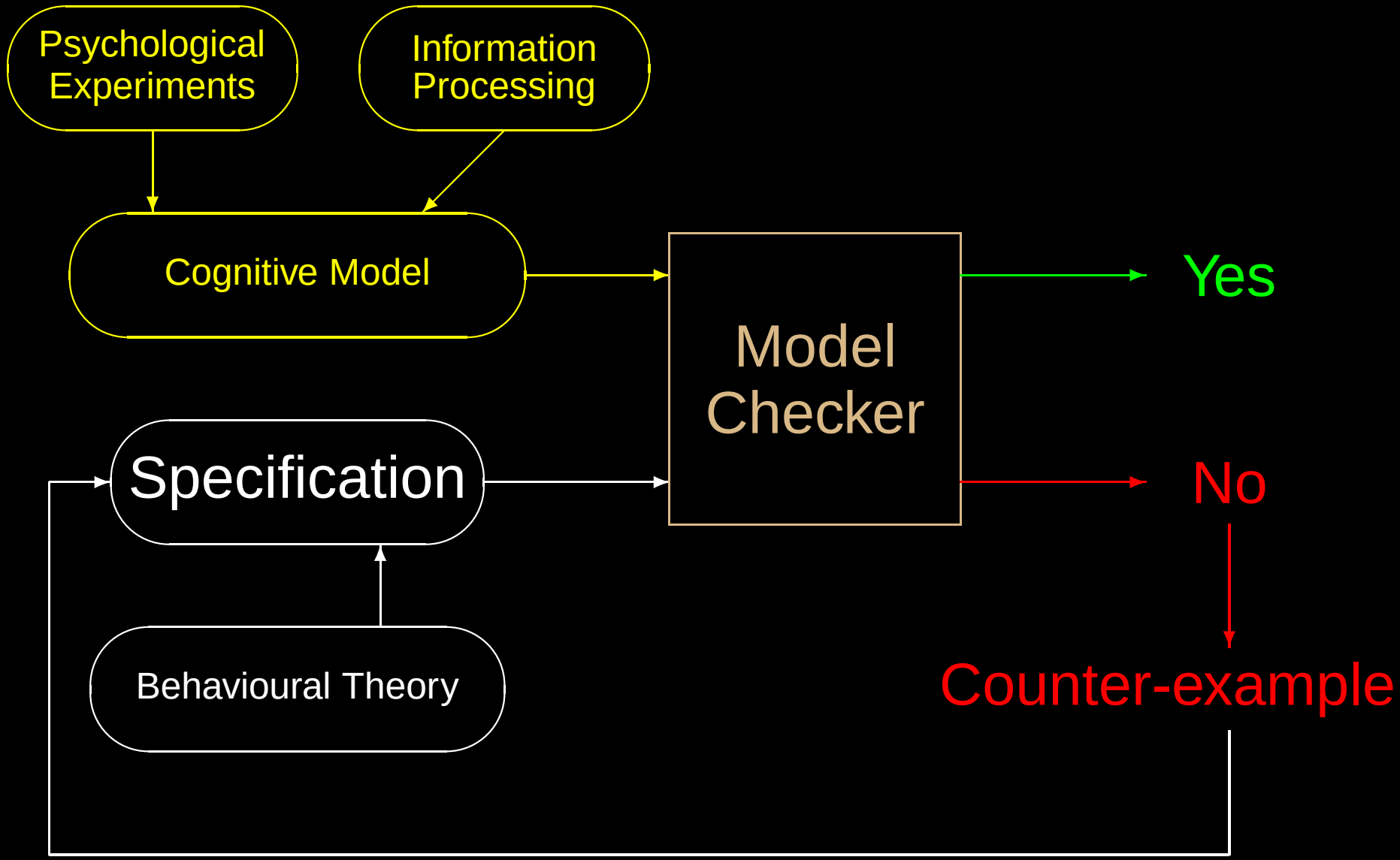
MC and Cognitive Psychology



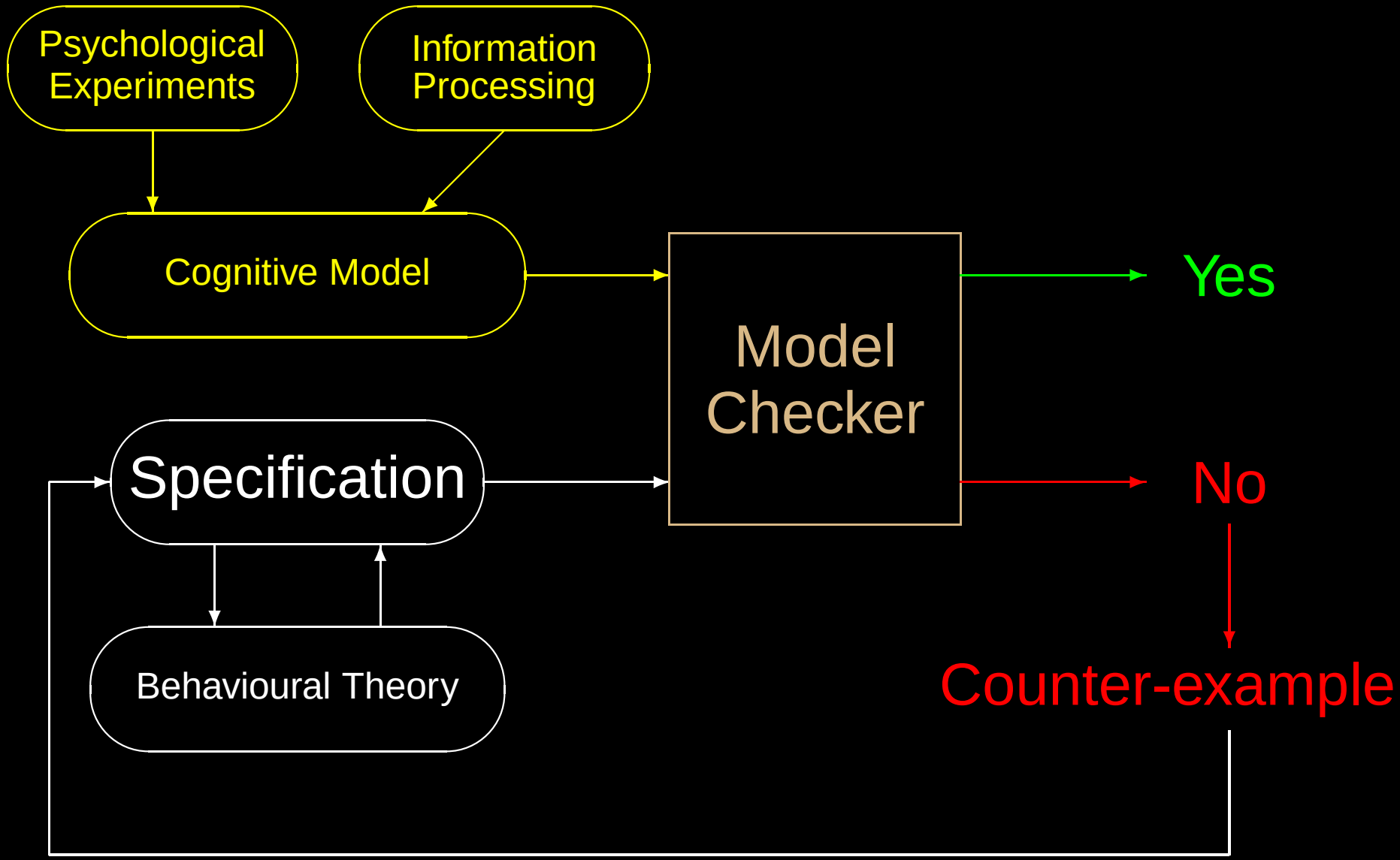
MC and Cognitive Psychology



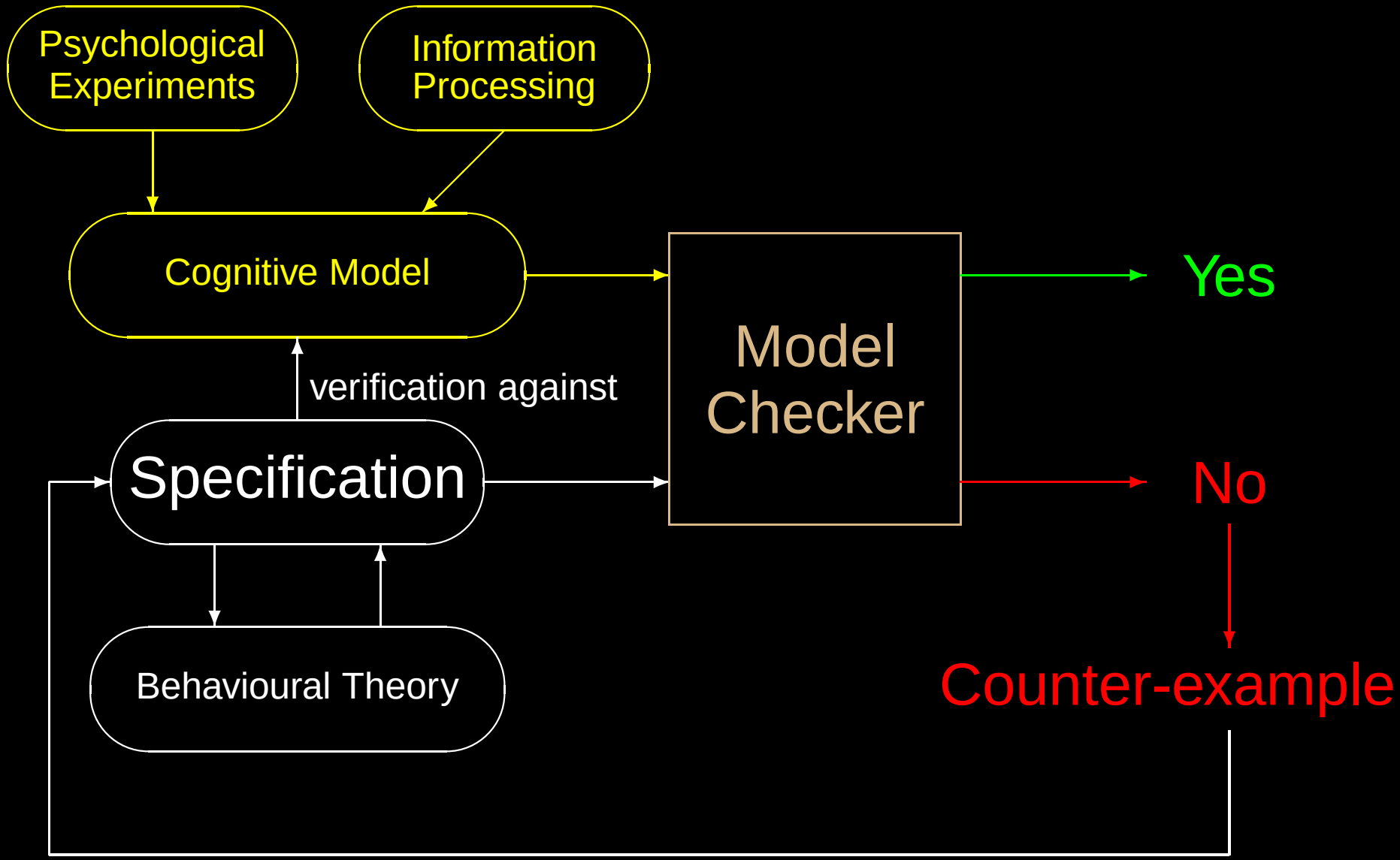
MC and Cognitive Psychology



MC and Cognitive Psychology



MC and Cognitive Psychology



Air Traffic Control (ATC)

- Aircraft fly along straight-line segments — called *flight paths* — between *waypoints* within a fixed sector of airspace.

Air Traffic Control (ATC)

- Aircraft fly along straight-line segments — called *flight paths* — between *waypoints* within a fixed sector of airspace.
- Aircraft *horizontal separation* must be at least 5 miles.

Air Traffic Control (ATC)

- Aircraft fly along straight-line segments — called *flight paths* — between *waypoints* within a fixed sector of airspace.
- Aircraft *horizontal separation* must be at least 5 miles.
- A *pair* of aircraft *violate separation* when the horizontal distance between them is less than 5 miles (*separation violation*).

Air Traffic Control (ATC)

- Aircraft fly along straight-line segments — called *flight paths* — between *waypoints* within a fixed sector of airspace.
- Aircraft *horizontal separation* must be at least 5 miles.
- A *pair* of aircraft *violate separation* when the horizontal distance between them is less than 5 miles (*separation violation*).
- A *pair* of aircraft is in *conflict* when their pathways are such that the two aircraft will eventually violate separation.

ATC Simulator

- The ATC operator's task involves monitoring the movement of aircraft on a screen, looking for pair of aircraft that *may violate separation*.

ATC Simulator

- The ATC operator's task involves monitoring the movement of aircraft on a screen, looking for pair of aircraft that *may violate separation*.
- When such a conflict is detected, the operator uses a mouse to select one of the aircraft and change its speed using a pulldown menu.

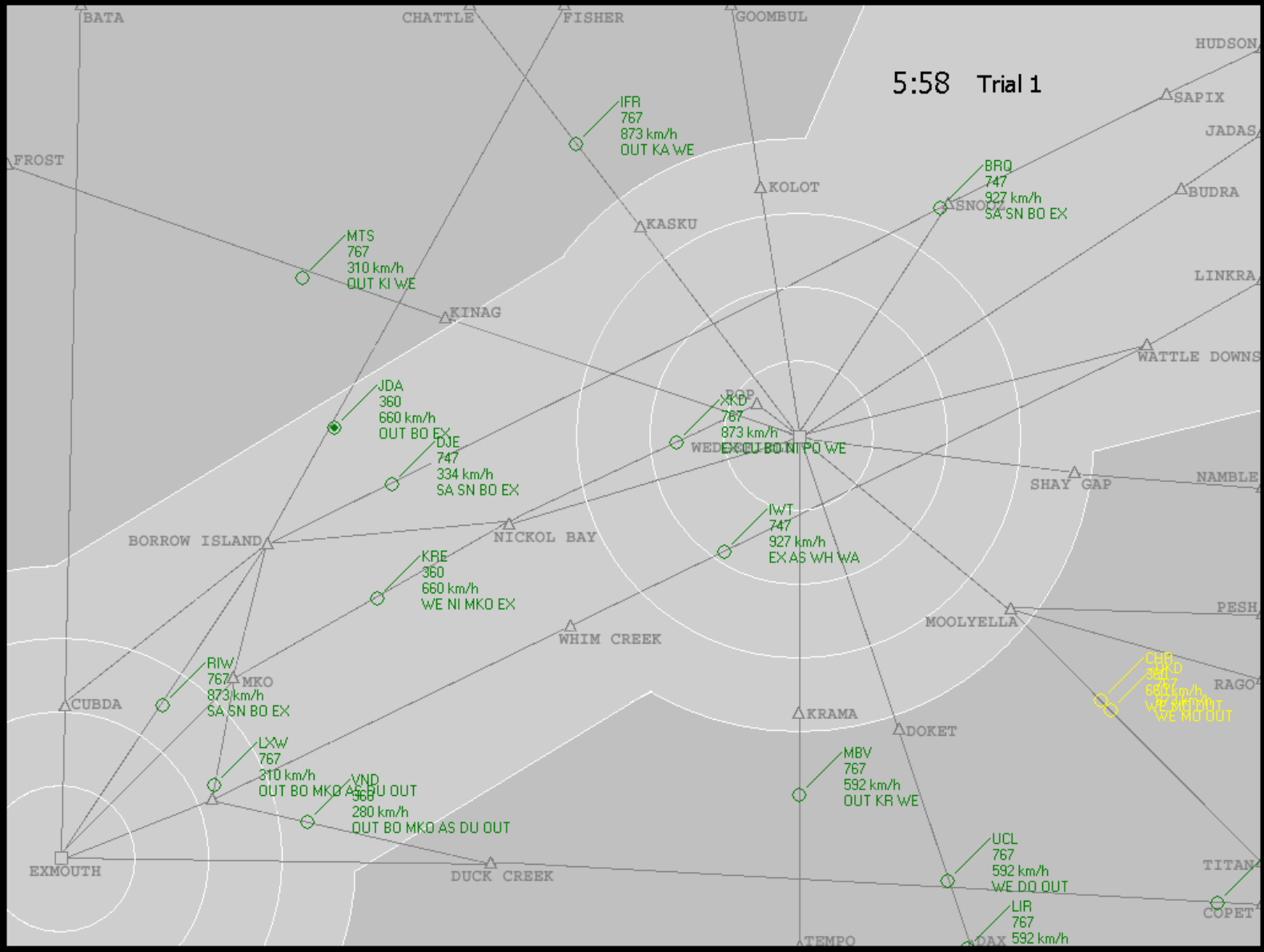
ATC Simulator

- The ATC operator's task involves monitoring the movement of aircraft on a screen, looking for pair of aircraft that *may violate separation*.
- When such a conflict is detected, the operator uses a mouse to select one of the aircraft and change its speed using a pulldown menu.
- The goal of the task is to resolve all conflicts before they violate separation, while not introducing any new conflict.

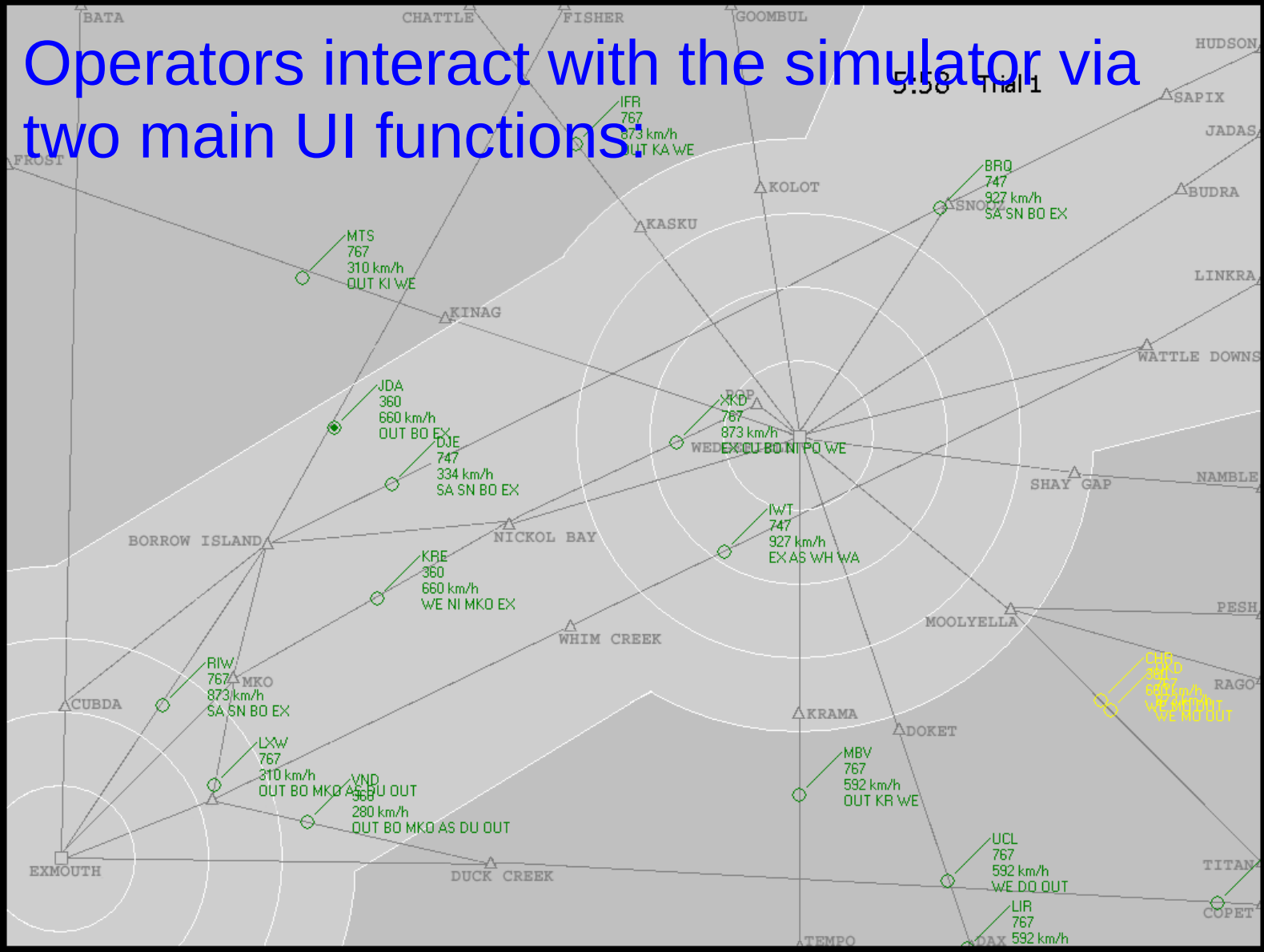
ATC Simulator

- The ATC operator's task involves monitoring the movement of aircraft on a screen, looking for pair of aircraft that *may violate separation*.
- When such a conflict is detected, the operator uses a mouse to select one of the aircraft and change its speed using a pulldown menu.
- The goal of the task is to resolve all conflicts before they violate separation, while not introducing any new conflict.
- We have a task failure when separation is violated.

ATC Simulator Screenshot



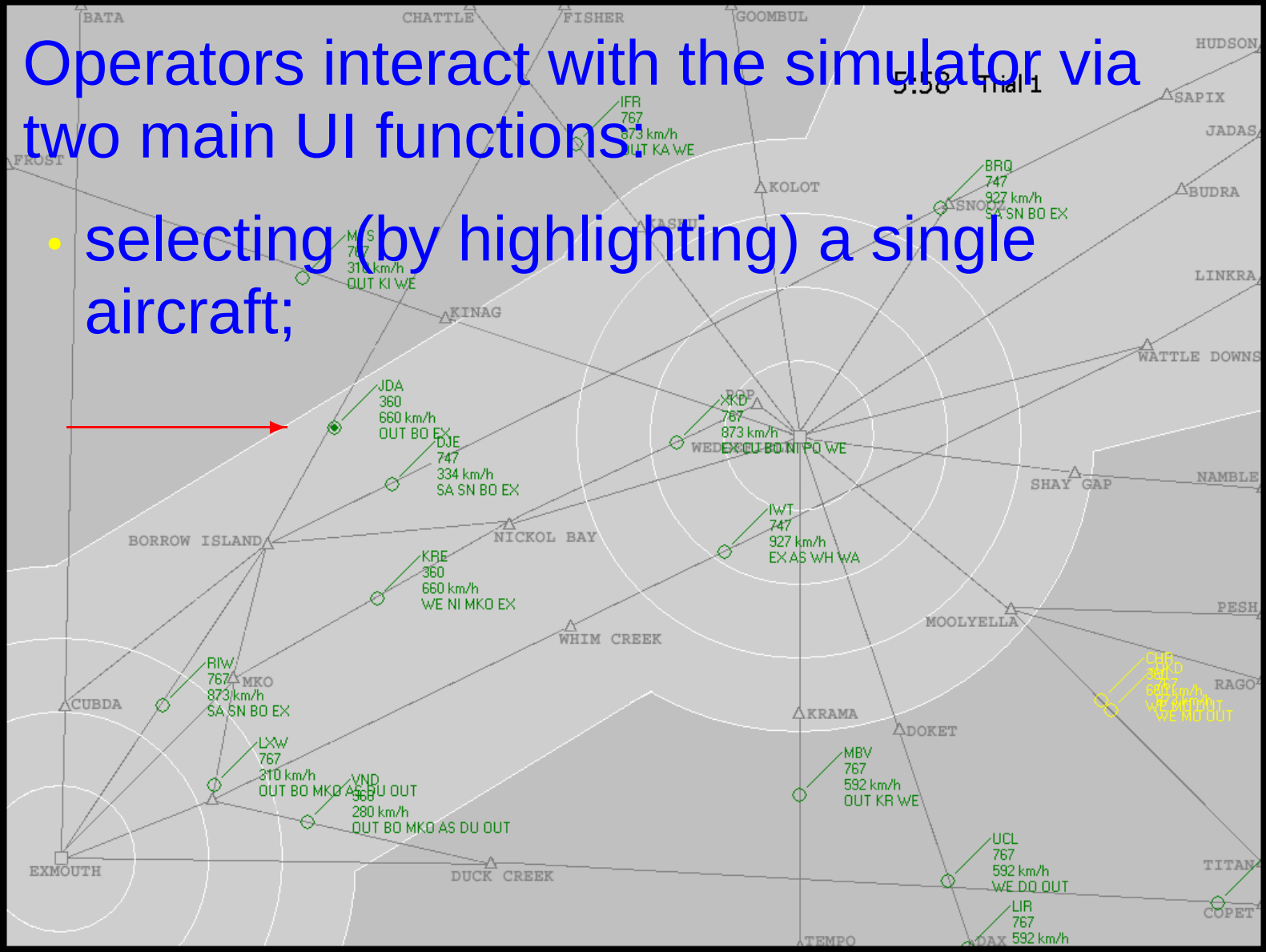
ATC Simulator Screenshot



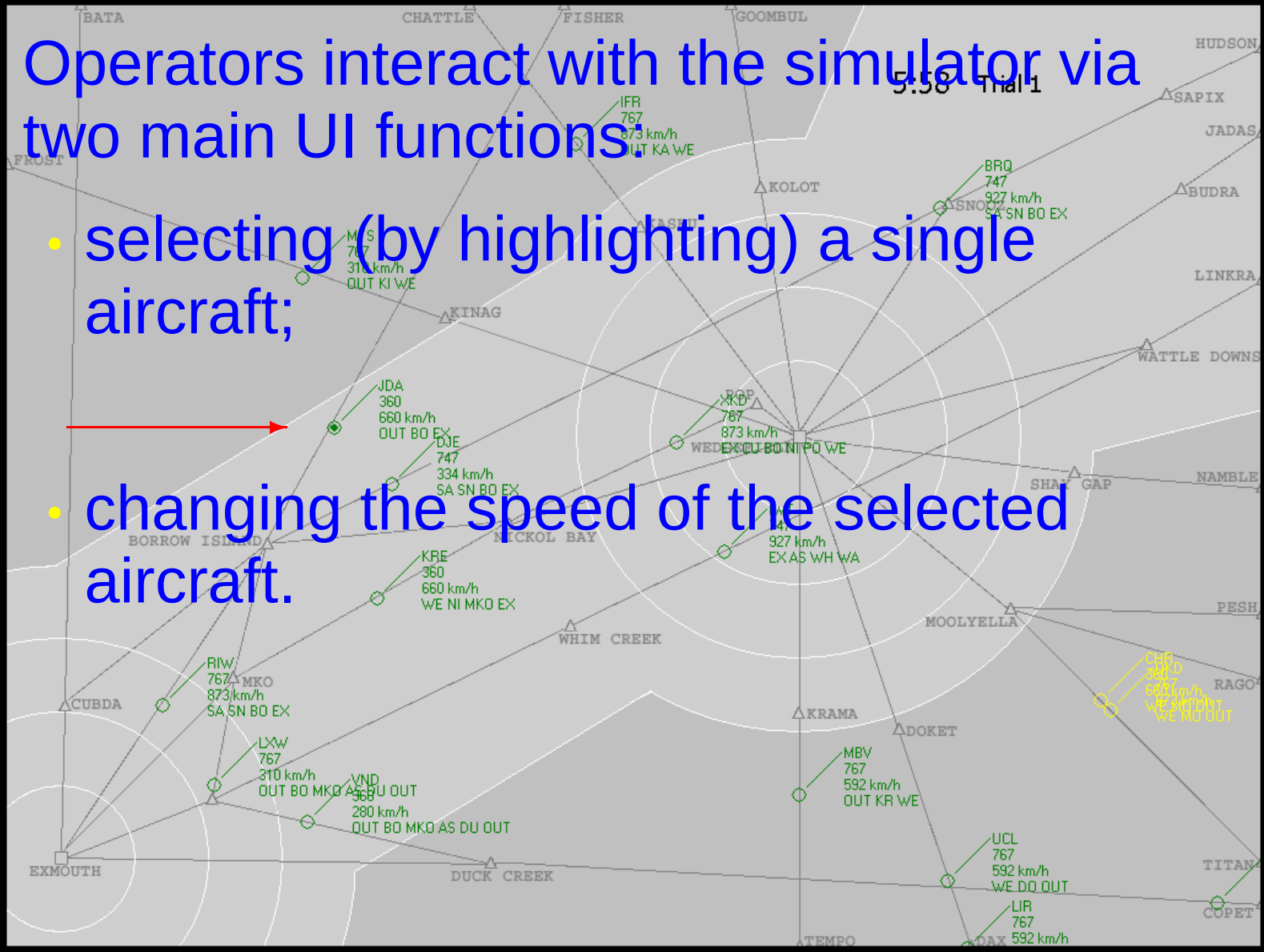
ATC Simulator Screenshot

Operators interact with the simulator via two main UI functions:

- selecting (by highlighting) a single aircraft;

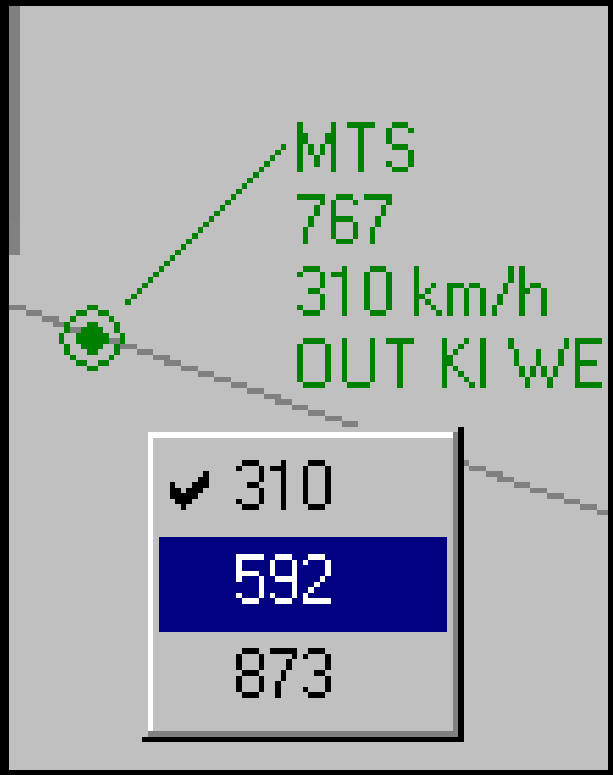


ATC Simulator Screenshot

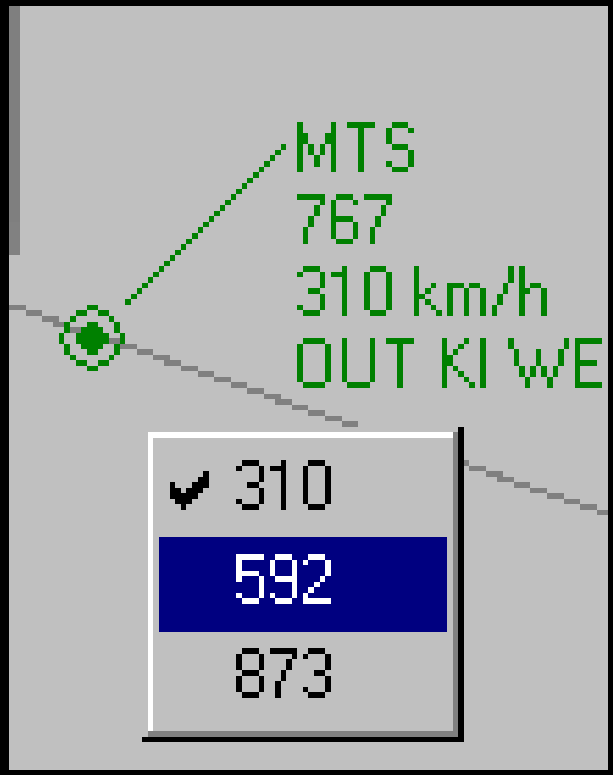


- Operators interact with the simulator via two main UI functions:
  - selecting (by highlighting) a single aircraft;
  - changing the speed of the selected aircraft.

Speed Menu

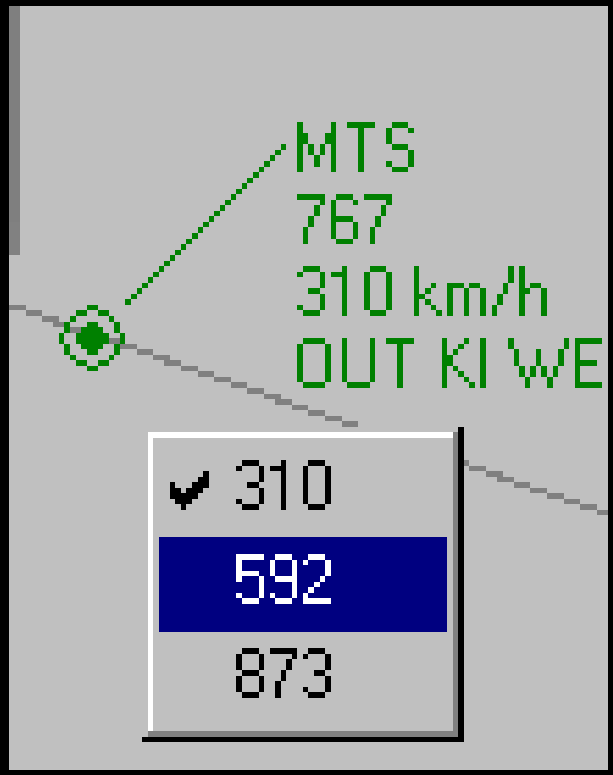


Speed Menu



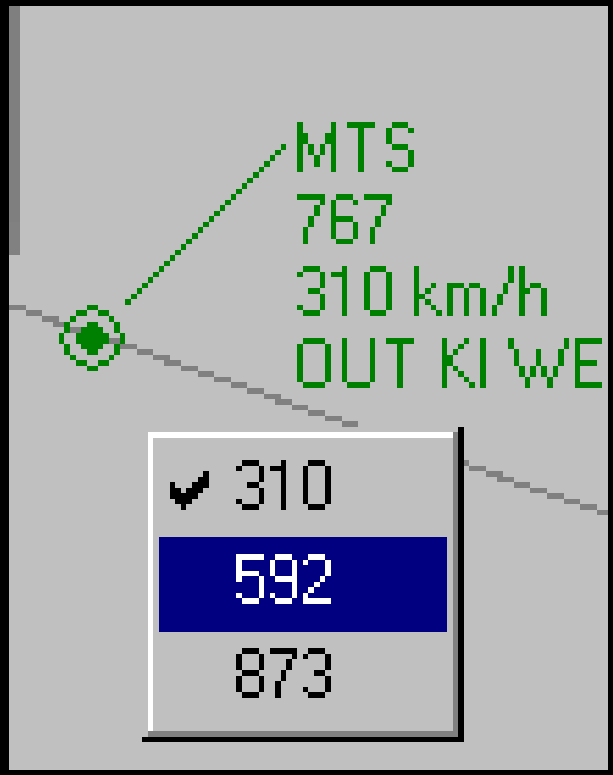
Open the menu by clicking the right button.

Speed Menu



Open the menu by clicking the right button.
The menu appears at the position of the cursor.

Speed Menu



Open the menu by clicking the right button.
The menu appears at the position of the cursor.
Selected the speed by left clicking on the desired menu entry.

Operator Erros

- slip: inadvertedly select a wrong or the current speed

Operator Erros

- slip: inadvertedly select a wrong or the current speed
  $\Longleftarrow$ selction task closure (cognitive problem)

Operator Erros

- slip: inadvertedly select a wrong or the current speed
  $\Longleftarrow$ selction task closure (cognitive problem)
- mistaken identity: change the spead of an aircraft different from the intended one

Operator Erros

- slip: inadvertedly select a wrong or the current speed
  $\Longleftarrow$ selction task closure (cognitive problem)
- mistaken identity: change the spead of an aircraft different from the intended one
  $\Longleftarrow$ the menu appears at the position of the cursor (usability problem)

Operator Erros

- slip: inadvertedly select a wrong or the current speed
  $\Longleftarrow$ selction task closure (cognitive problem)
- mistaken identity: change the spead of an aircraft different from the intended one
  $\Longleftarrow$ the menu appears at the position of the cursor (usability problem)
- mis-classification, mis-prioritization, conflict generation

Operator Erros

- slip: inadvertedly select a wrong or the current speed
  $\Longleftarrow$ selction task closure (cognitive problem)
- mistaken identity: change the spead of an aircraft different from the intended one
  $\Longleftarrow$ the menu appears at the position of the cursor (usability problem)
- mis-classification, mis-prioritization, conflict generation

The operator can recover from these errors without causing separation violation (task failure)

OCM for Air Traffic Control

Scanning: The operator scans among each pair of aircraft searching for a pair that may violate separation.

Identification: The operator identifies a pair of aircraft.

Classification: The operator

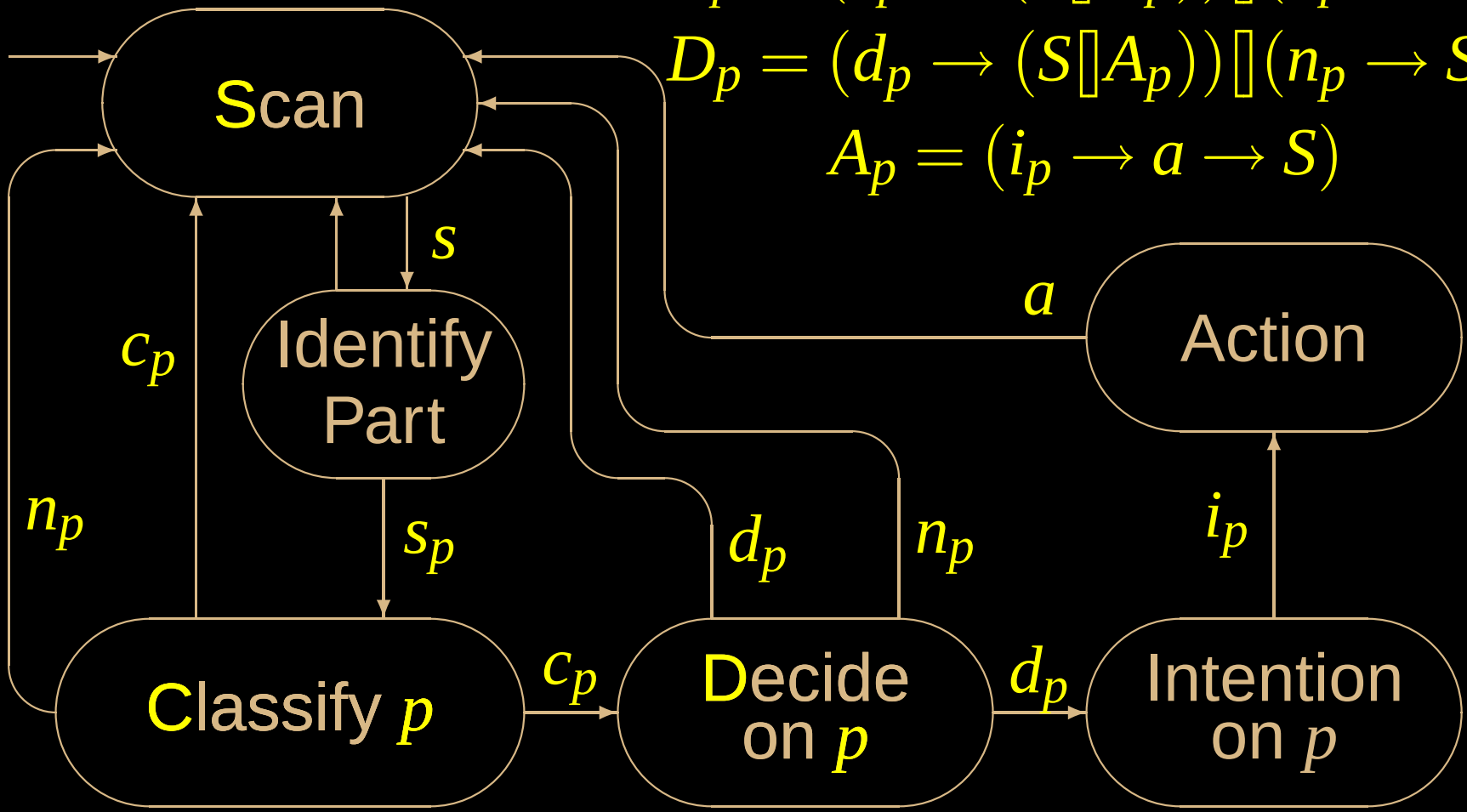
- assesses whether the identified pair of aircraft will eventually violate separation (in conflict) or not (not in conflict);
- if so, gives a priority to the conflict according to its urgency to be resolved.

Decision on how to resolve the conflict.

Action to be performed as a series of interaction with the interface.

Model Interpretation for ATC

$$S = s \rightarrow (([]_{p:Part}(s_p \rightarrow C_p))[]S)$$
$$C_p = (c_p \rightarrow (S[]D_p))[](n_p \rightarrow S)$$
$$D_p = (d_p \rightarrow (S[]A_p))[](n_p \rightarrow S)$$
$$A_p = (i_p \rightarrow a \rightarrow S)$$



Model Interpretation for ATC

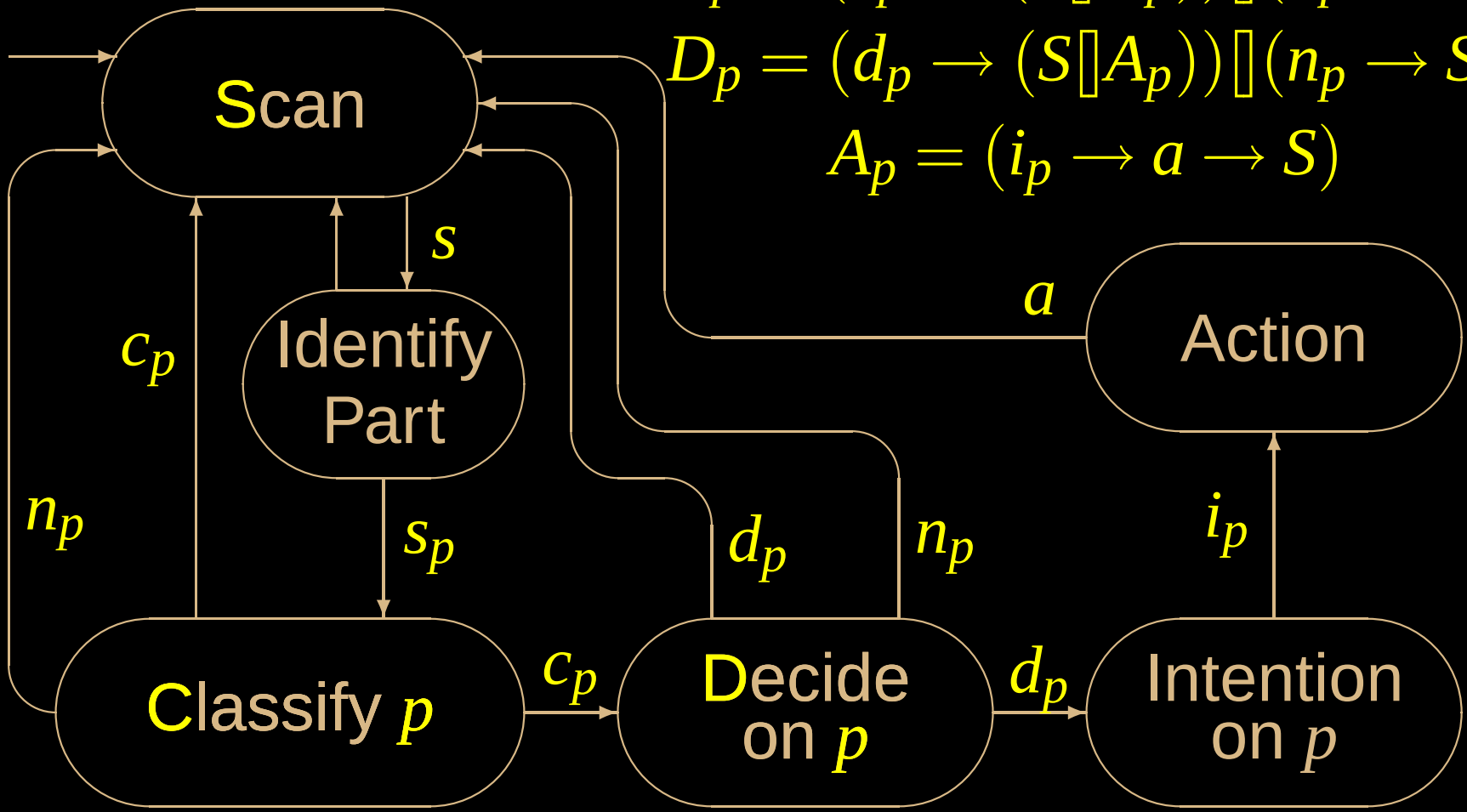
$p =$ Pair of aircraft

$$S = s \rightarrow (([]_{p:Pairs}(s_p \rightarrow C_p))[]S)$$

$$C_p = (c_p \rightarrow (S[]D_p))[](n_p \rightarrow S)$$

$$D_p = (d_p \rightarrow (S[]A_p))[](n_p \rightarrow S)$$

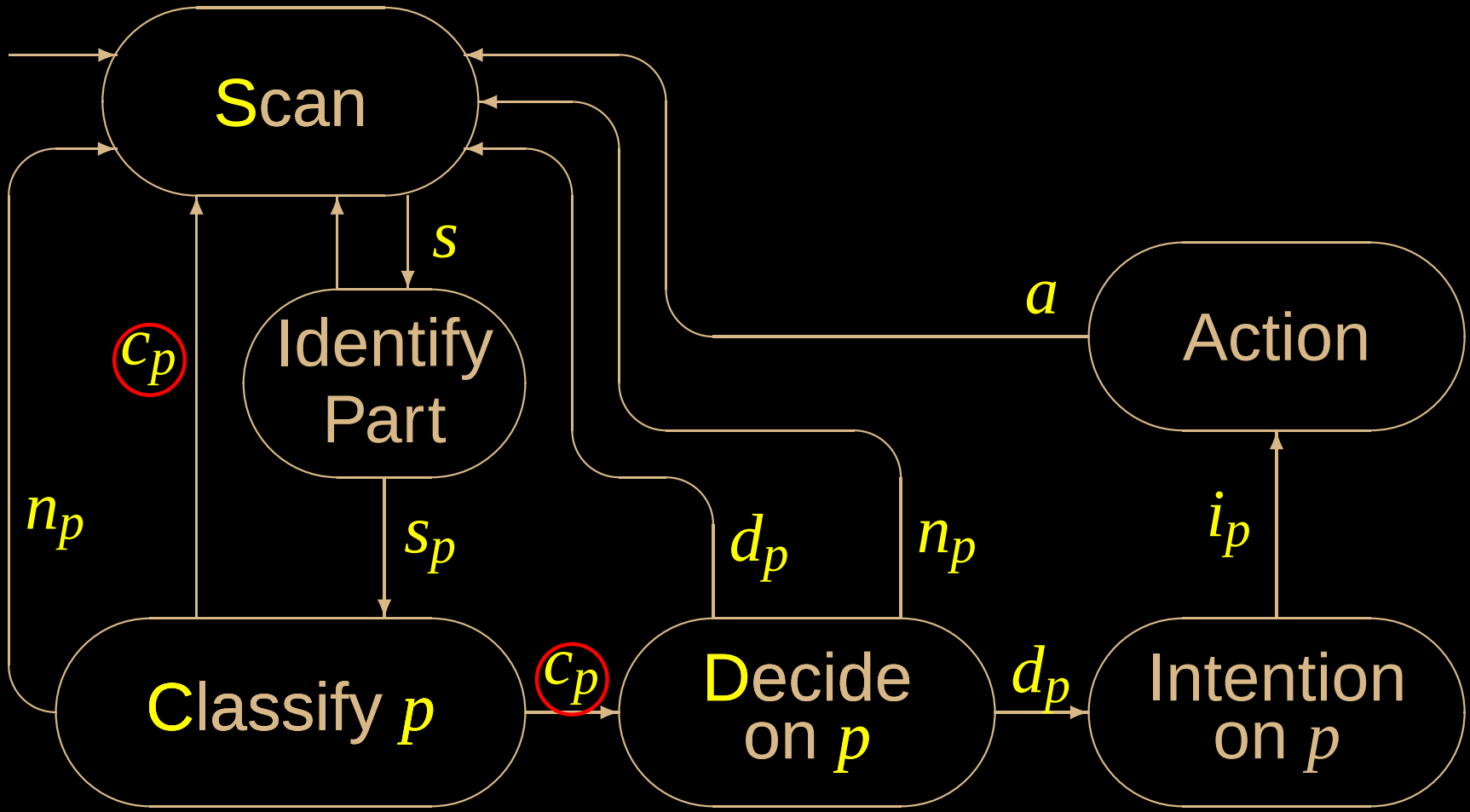
$$A_p = (i_p \rightarrow a \rightarrow S)$$



Model Interpretation for ATC

$p =$ Pair of aircraft

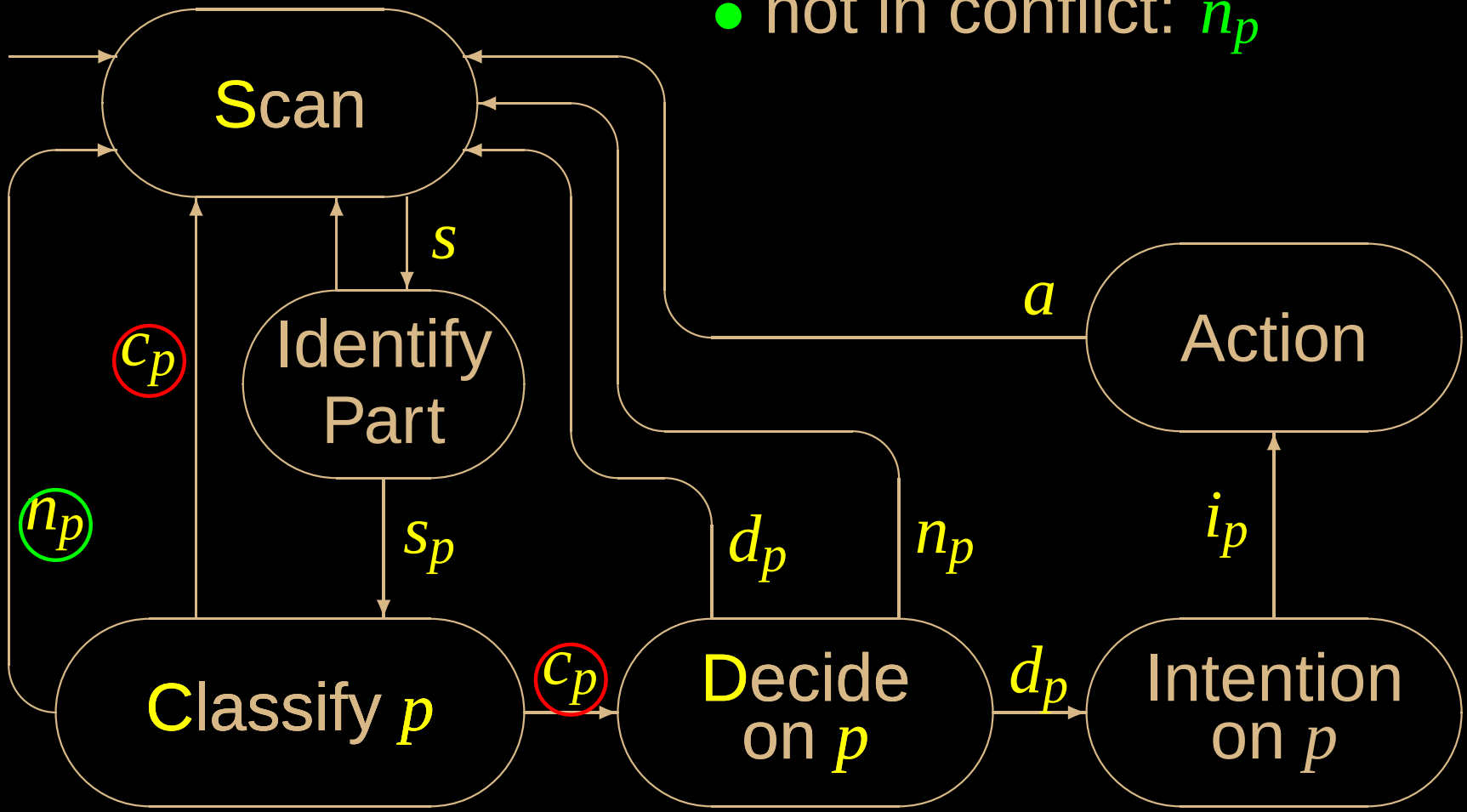
The pair is classified
- in conflict: c_p



Model Interpretation for ATC

$p =$ Pair of aircraft

The pair is classified
- in conflict: c_p
- not in conflict: n_p

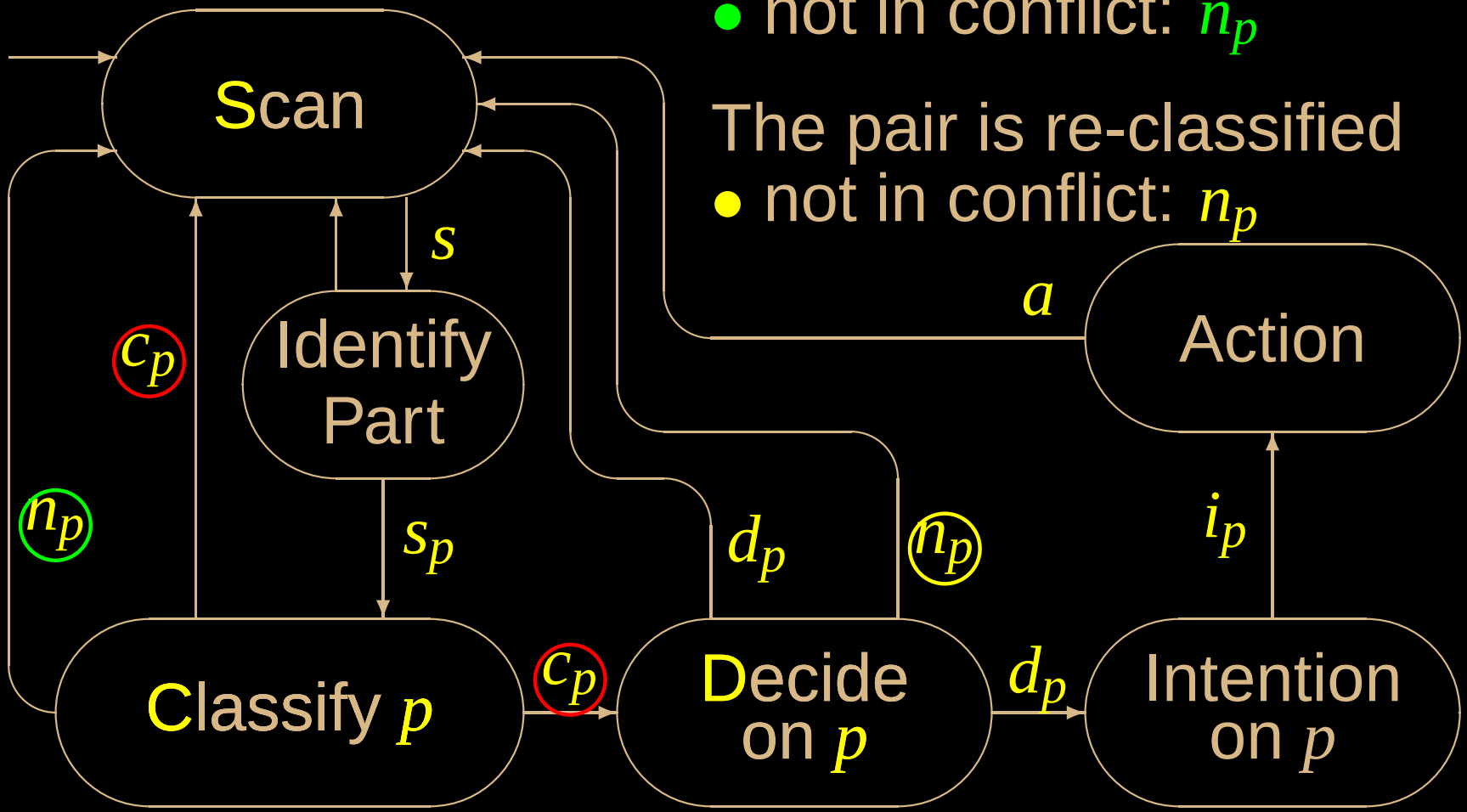


Model Interpretation for ATC

$p =$ Pair of aircraft

The pair is classified
- in conflict: c_p
- not in conflict: n_p

The pair is re-classified
- not in conflict: n_p



OCM for Air Traffic Control

Scanning: The operator scans among each pair of aircraft searching for a pair that may violate separation.

Identification: The operator identifies a pair of aircraft.

Classification: The operator

- assesses whether the identified pair of aircraft will eventually violate separation (in conflict) or not (not in conflict);
- if so, gives a priority to the conflict according to its urgency to be resolved.

Decision on how to resolve the conflict.

Action to be performed as a series of interaction with the interface.

Environment Model

$$
\begin{aligned}
S &= s \rightarrow (([]_{p:Pairs}(s_p \rightarrow C_p))[]S) \\
C_p &= (c_p \rightarrow (S[]D_p))[](n_p \rightarrow S) \\
D_p &= (d_p \rightarrow (S[]A_p))[](n_p \rightarrow S) \\
A_p &= (i_p \rightarrow a \rightarrow S)
\end{aligned}
$$

Environment Model

$$
\begin{aligned}
S &= s \rightarrow ((\Box_{p:Pairs}(s_p \rightarrow C_p)) \Box S) \\
C_p &= (c_p \rightarrow (S \Box D_p)) \Box (n_p \rightarrow S) \\
D_p &= (d_p \rightarrow (S \Box A_p)) \Box (n_p \rightarrow S) \\
A_p &= (i_p \rightarrow a \rightarrow S)
\end{aligned}
$$

$$
\begin{aligned}
I_p = s \rightarrow a \rightarrow ((&(unresolved_p \rightarrow I_p) \Box \\
&(resolved_p \rightarrow N_p) \Box \\
&(noeffect_p \rightarrow I_p))
\end{aligned}
$$

Environment Model

$$
\begin{aligned}
S &= s \rightarrow (([]_{p:Pairs}(s_p \rightarrow C_p))[]S) \\
C_p &= (c_p \rightarrow (S[]D_p))[](n_p \rightarrow S) \\
D_p &= (d_p \rightarrow (S[]A_p))[](n_p \rightarrow S) \\
A_p &= (i_p \rightarrow a \rightarrow S)
\end{aligned}
$$

$$
\begin{aligned}
I_p = s \rightarrow a \rightarrow ((&(unresolved_p \rightarrow I_p)[] \\
&(resolved_p \rightarrow N_p)[] \\
&(noeffect_p \rightarrow I_p))
\end{aligned}
$$

$$
\begin{aligned}
N_p = s \rightarrow a \rightarrow ((&(unnecessary_p \rightarrow N_p)[] \\
&(adverse_p \rightarrow I_p)[] \\
&(noeffect_p \rightarrow N_p))
\end{aligned}
$$

Environment Model

$$
\begin{aligned}
S &= s \rightarrow ((\Box_{p:Pairs}(s_p \rightarrow C_p)) \Box S) \\
C_p &= (c_p \rightarrow (S \Box D_p)) \Box (n_p \rightarrow S) \\
D_p &= (d_p \rightarrow (S \Box A_p)) \Box (n_p \rightarrow S) \\
A_p &= (i_p \rightarrow a \rightarrow S)
\end{aligned}
$$

$$
\begin{aligned}
I_p = s \rightarrow a \rightarrow ((&(unresolved_p \rightarrow I_p) \Box \\
&(resolved_p \rightarrow N_p) \Box \\
&(noeffect_p \rightarrow I_p))
\end{aligned}
$$

$$
\begin{aligned}
N_p = s \rightarrow a \rightarrow ((&(unnecessary_p \rightarrow N_p) \Box \\
&(adverse_p \rightarrow I_p) \Box \\
&(noeffect_p \rightarrow N_p))
\end{aligned}
$$

$$OCM = S \parallel (\parallel_{p:Init_I} I_p) \parallel (\parallel_{p:Init_N} N_p)$$

Task Failure Analysis

Three levels of decomposition of task failures.

Task Failure Analysis

Three levels of decomposition of task failures.

A first decomposition of task failures is based on

- the intention of the operator to resolve a conflict (i_p);

Task Failure Analysis

Three levels of decomposition of task failures.

A first decomposition of task failures is based on

- the intention of the operator to resolve a conflict (i_p);

and on the result, benign or adverse, of the operator's action:

Task Failure Analysis

Three levels of decomposition of task failures.

A first decomposition of task failures is based on

- the intention of the operator to resolve a conflict (i_p);

and on the result, benign or adverse, of the operator's action:

- the fact that the initial conflict I_p is effectively resolved ($resolved_p$);

Task Failure Analysis

Three levels of decomposition of task failures.

A first decomposition of task failures is based on

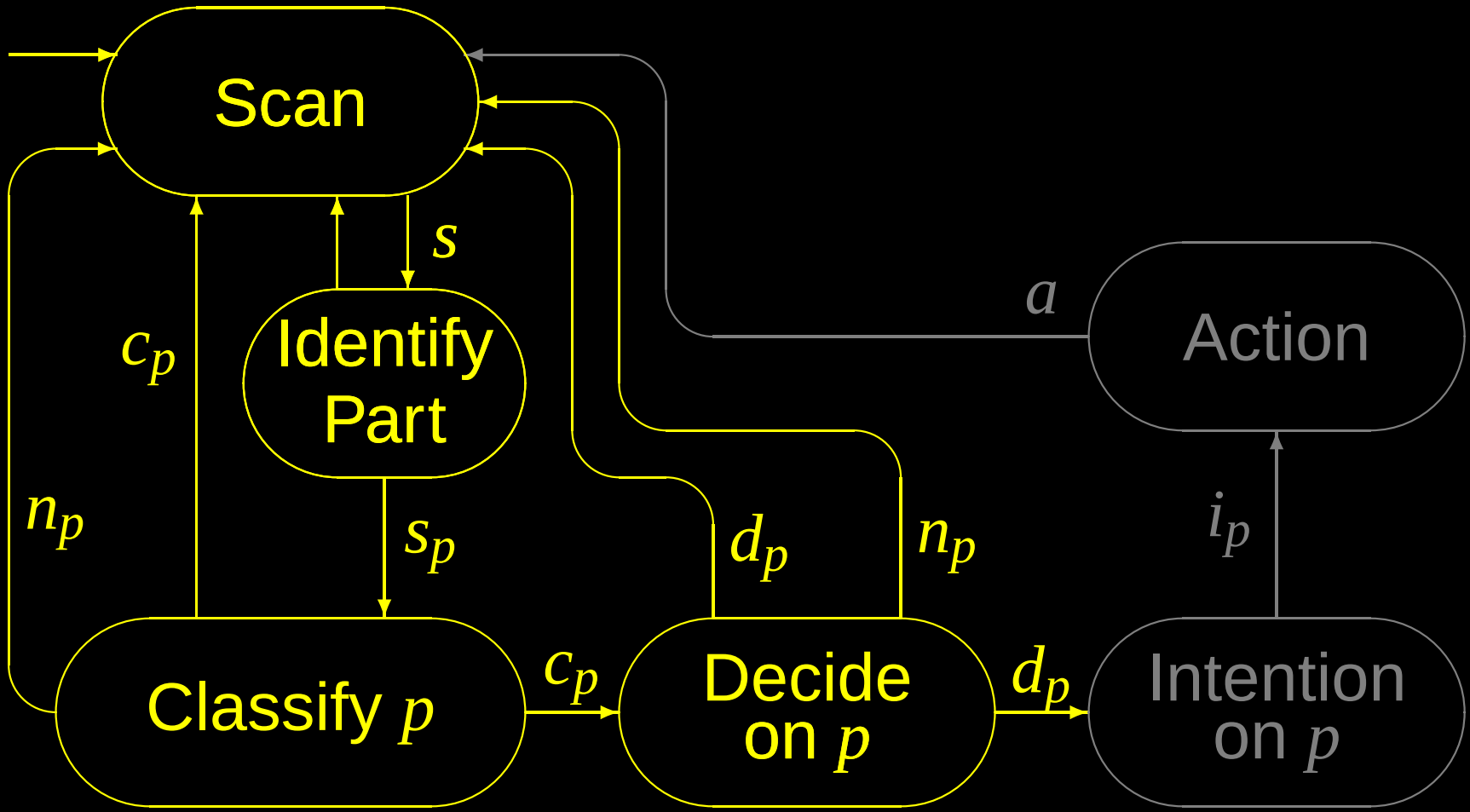
- the intention of the operator to resolve a conflict (i_p);

and on the result, benign or adverse, of the operator's action:

- the fact that the initial conflict I_p is effectively resolved ($resolved_p$);
- the fact that in absence of initial conflict (N_p) a new conflict is created ($adverse_p$).

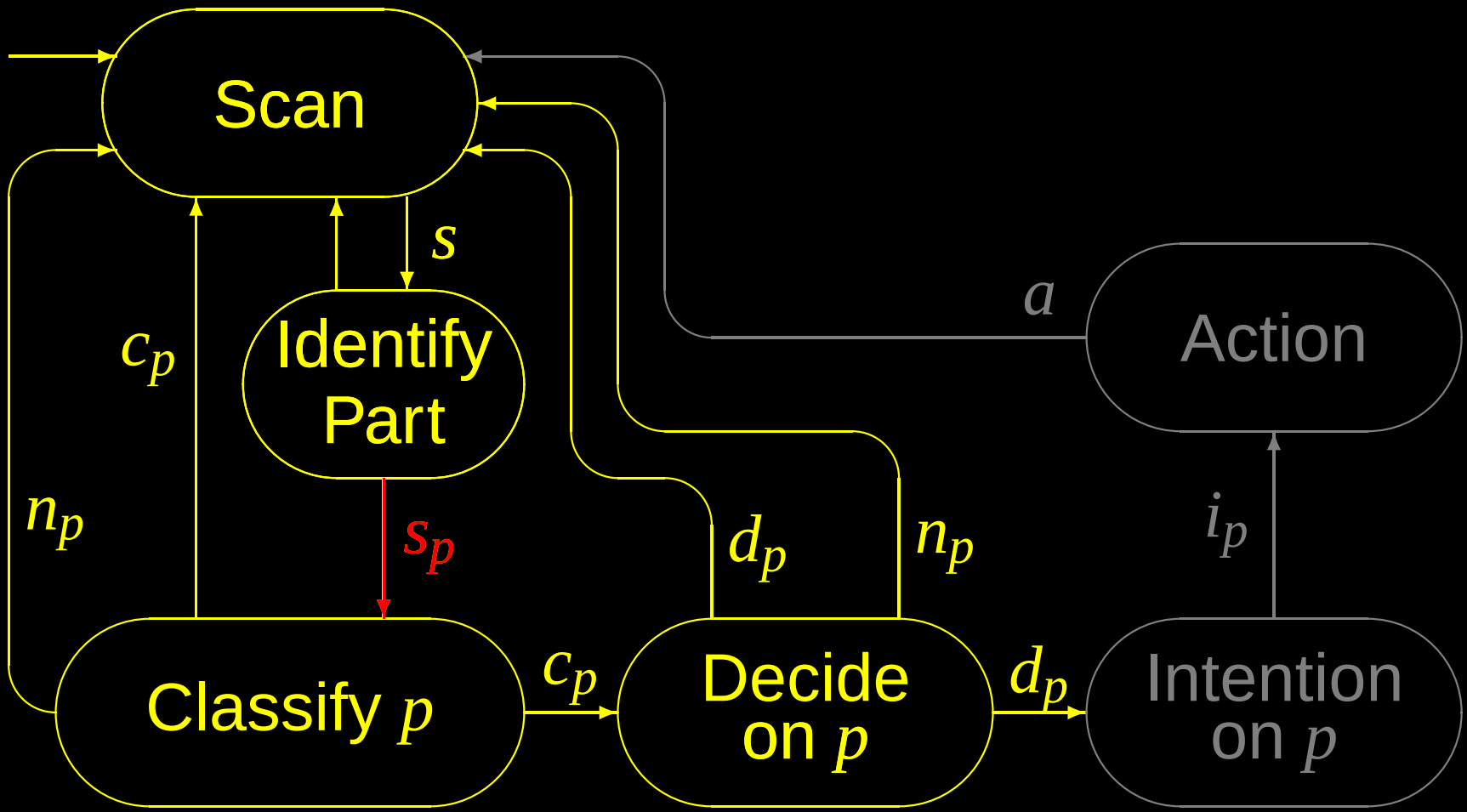
Failure of Scanning

no_intended_response$_p$:



Failure of Scanning

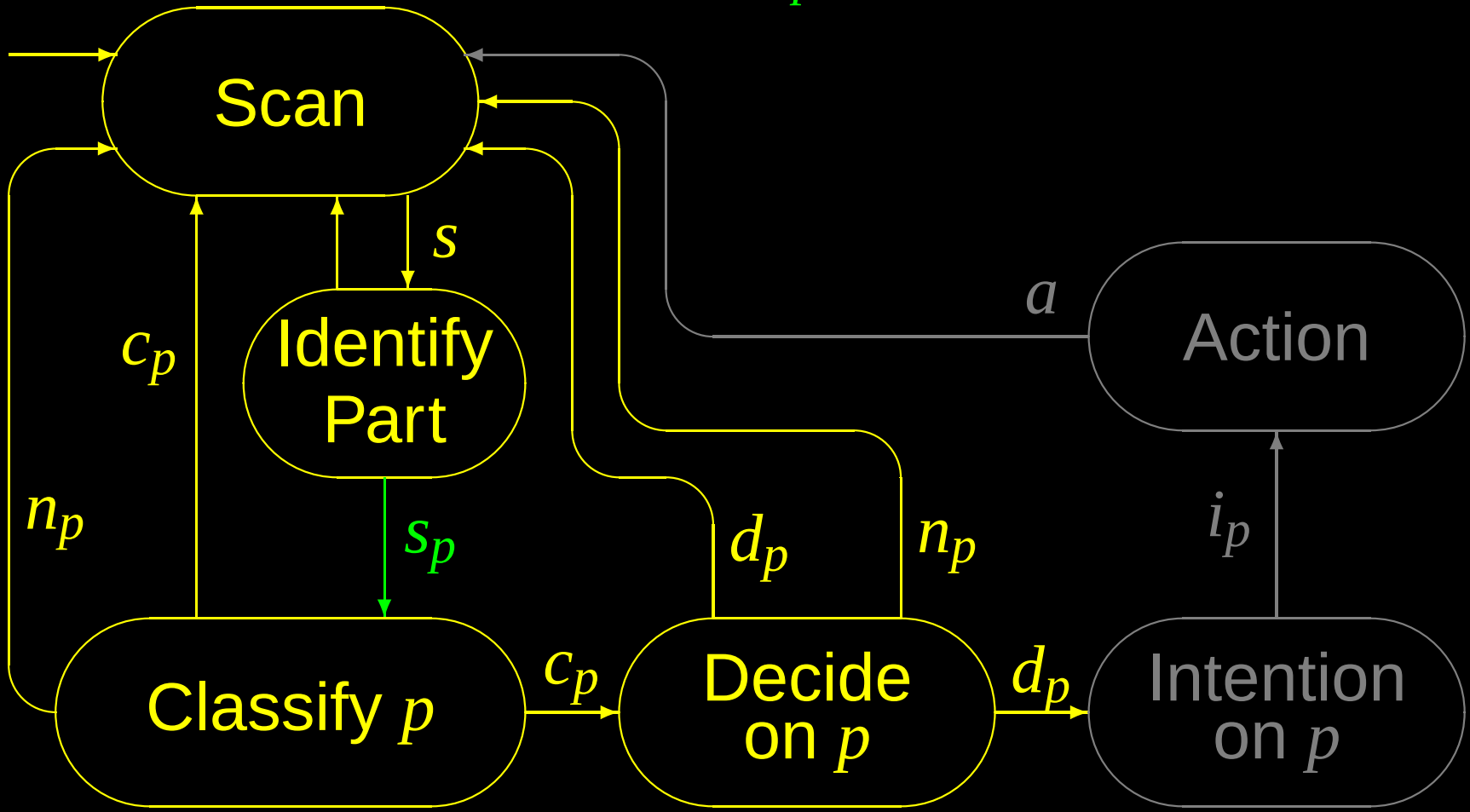
$no\_intended\_response_p$: $\Box \neg s_p$



Failure of Making Decision

$no\_intended\_response_p$: $\Box \neg s_p$

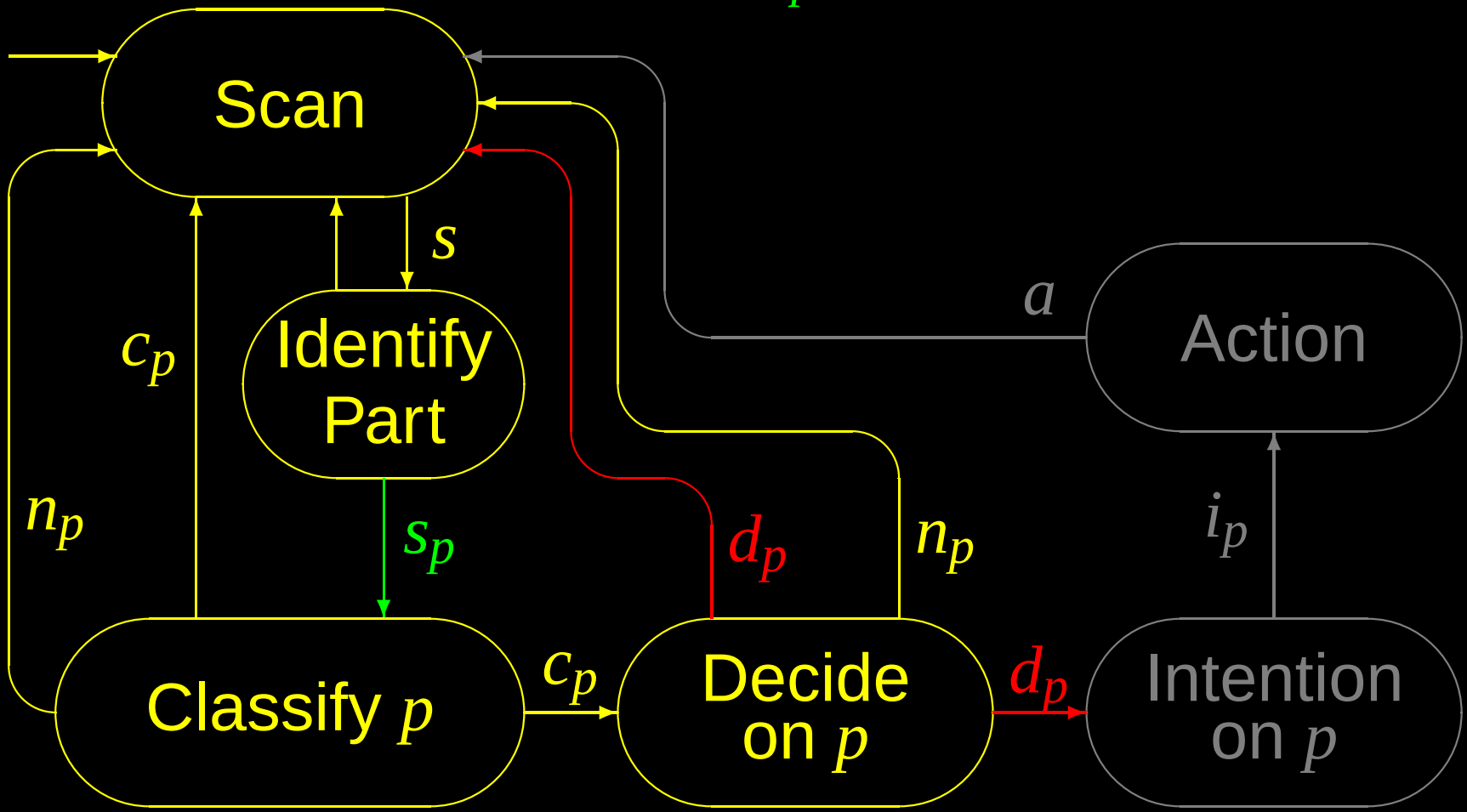
$\Diamond s_p \wedge \ldots$



Failure of Making Decision

$no\_intended\_response_p$: $\Box\neg\, s_p$

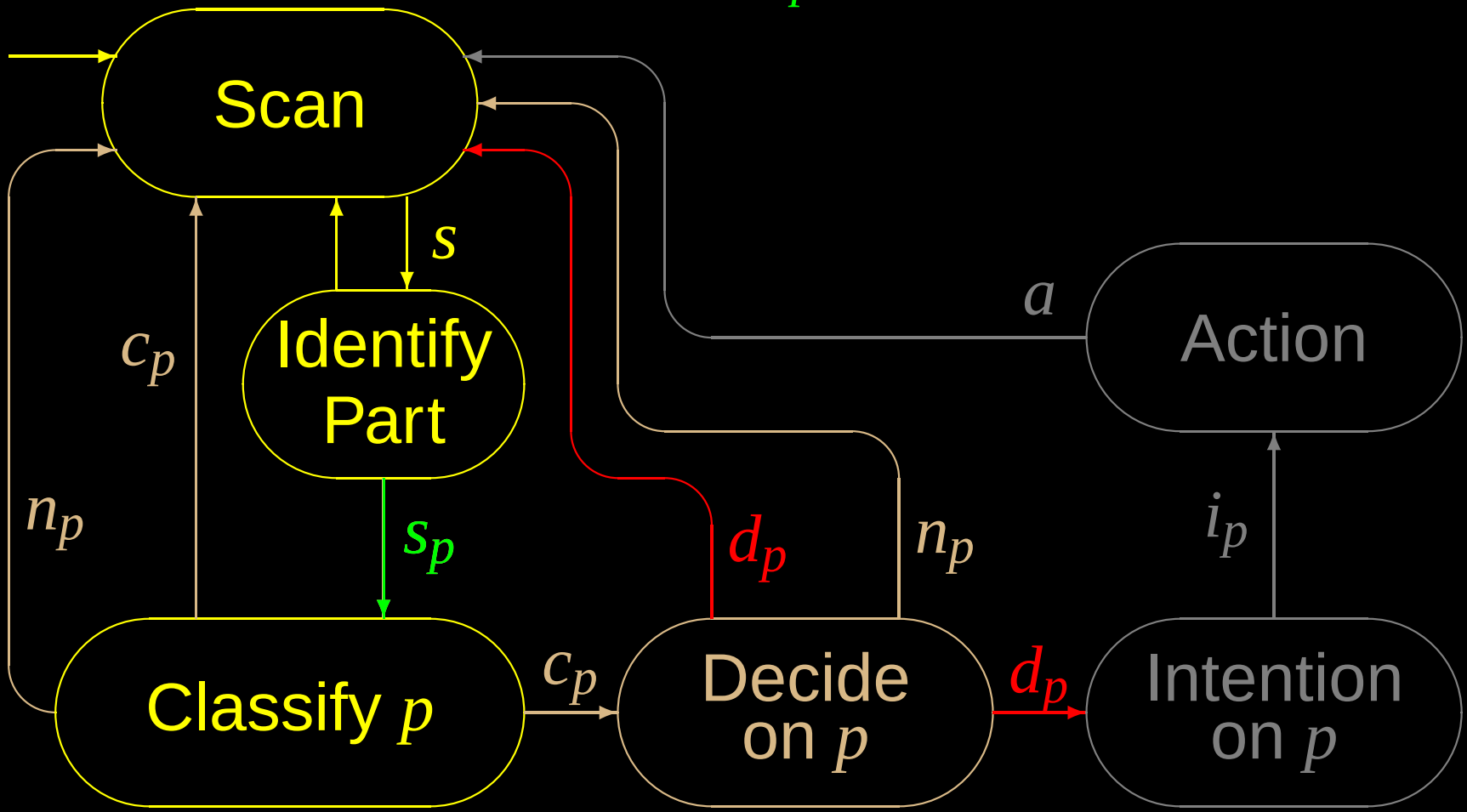
$\Diamond s_p \wedge \ldots$



Persistent Mis-classification

$no\_intended\_response_p$: $\Box\neg\, s_p$

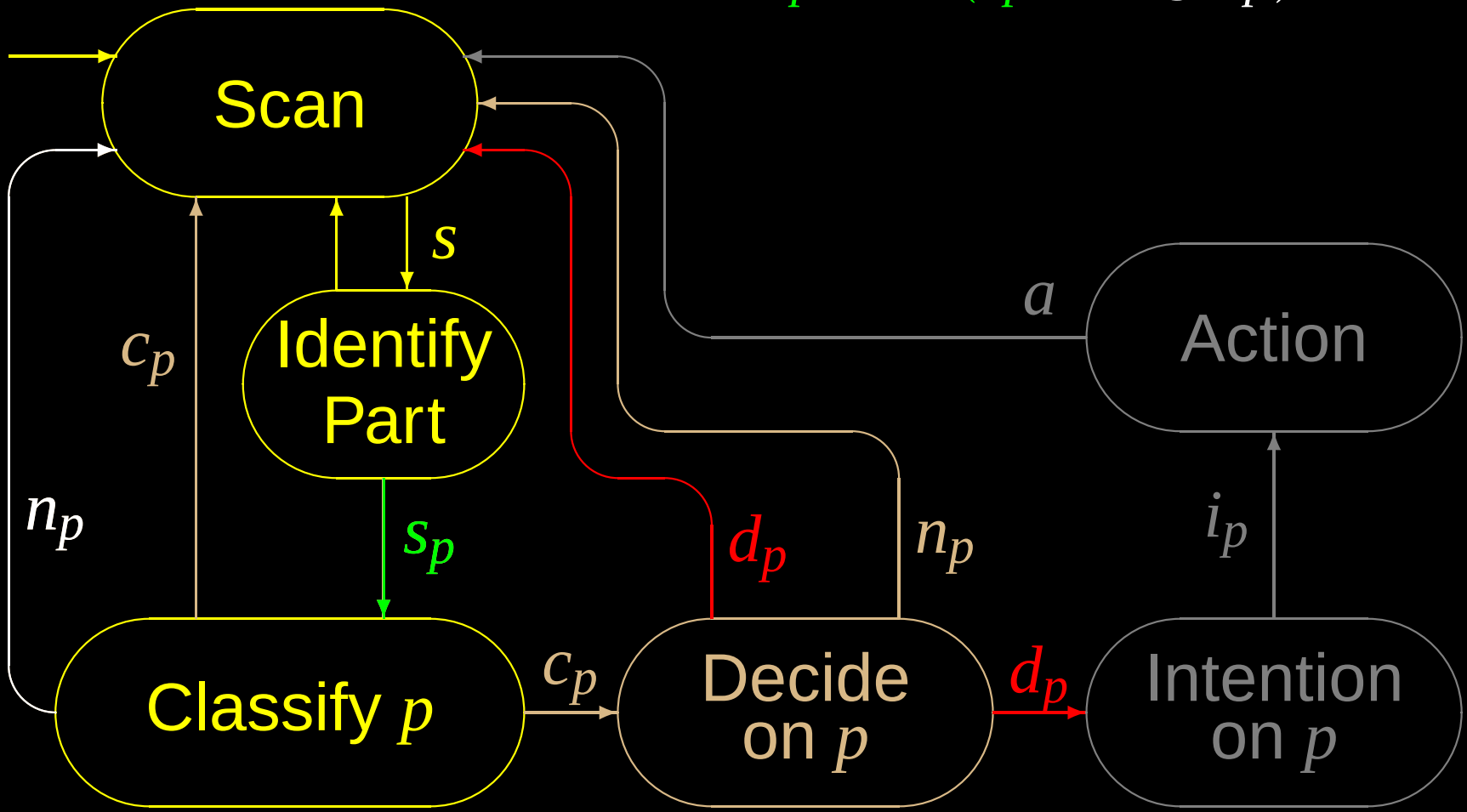
$\Diamond s_p \wedge \ldots$



Persistent Mis-classification

$no\_intended\_response_p$: $\Box\neg\, s_p$

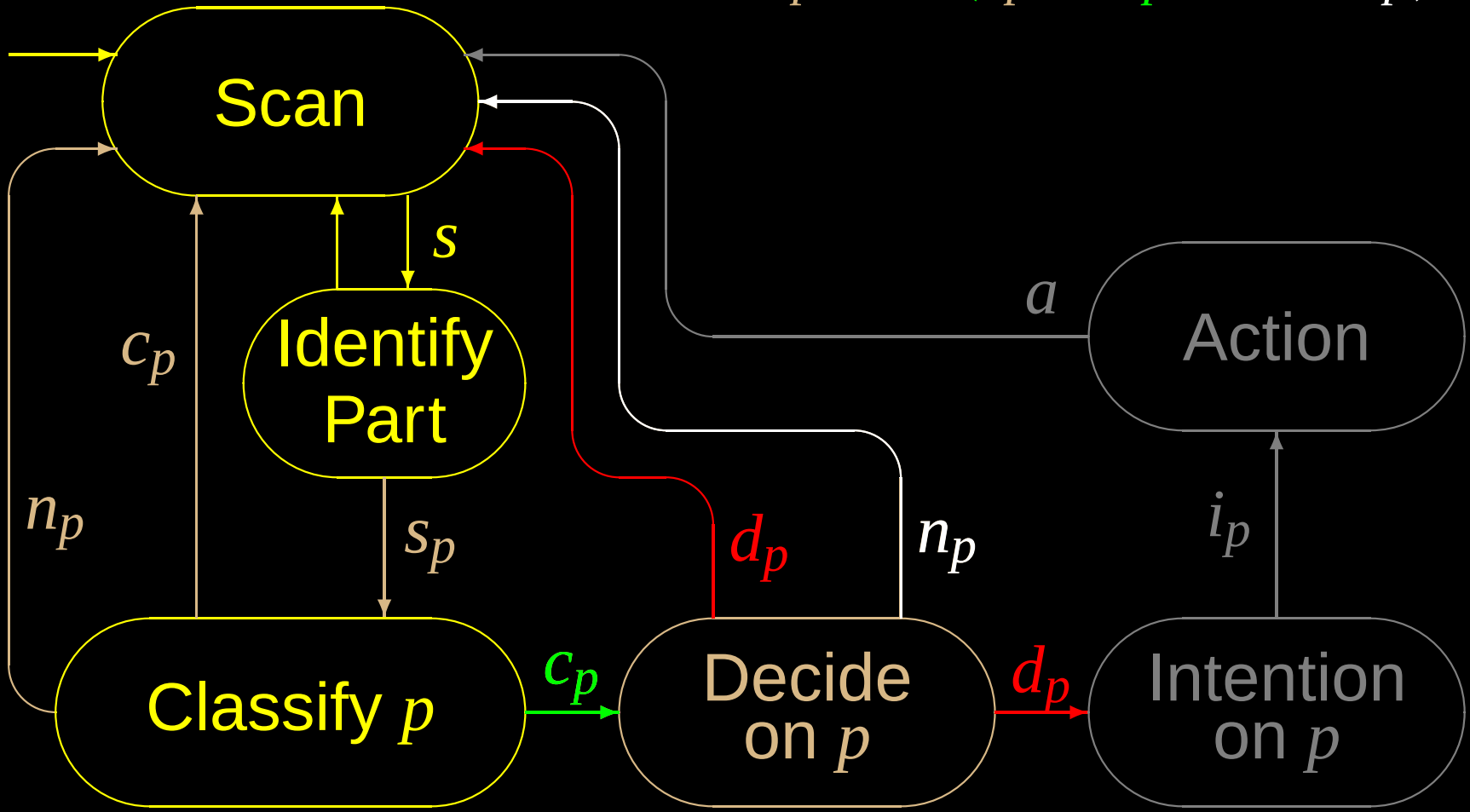
$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$



Persistent Mis-classification

no_intended_response$_p$: $\Box\neg\, s_p$

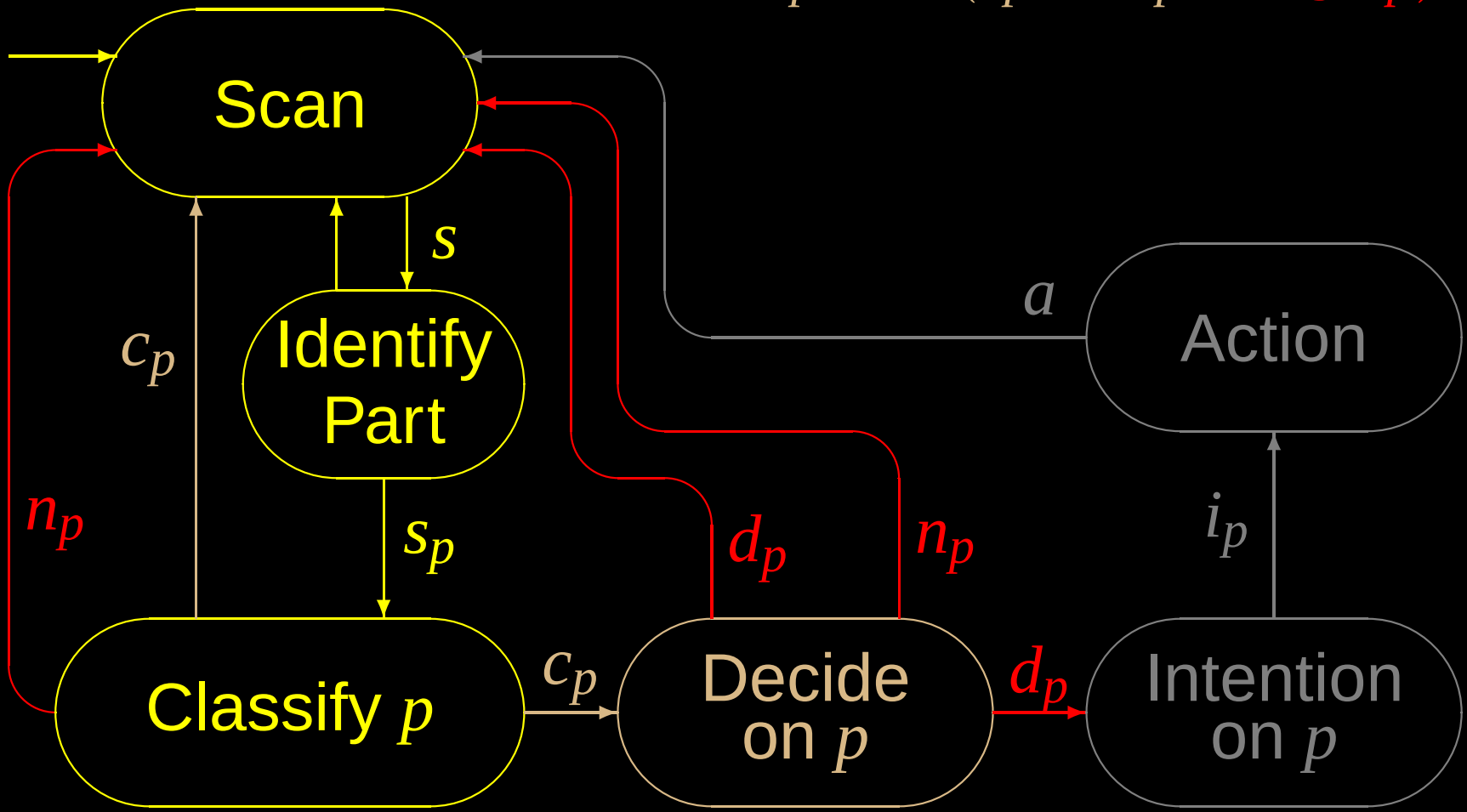
$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$



Persistent Mis-prioritisation

$no\_intended\_response_p$: $\Box\neg\, s_p$

$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$



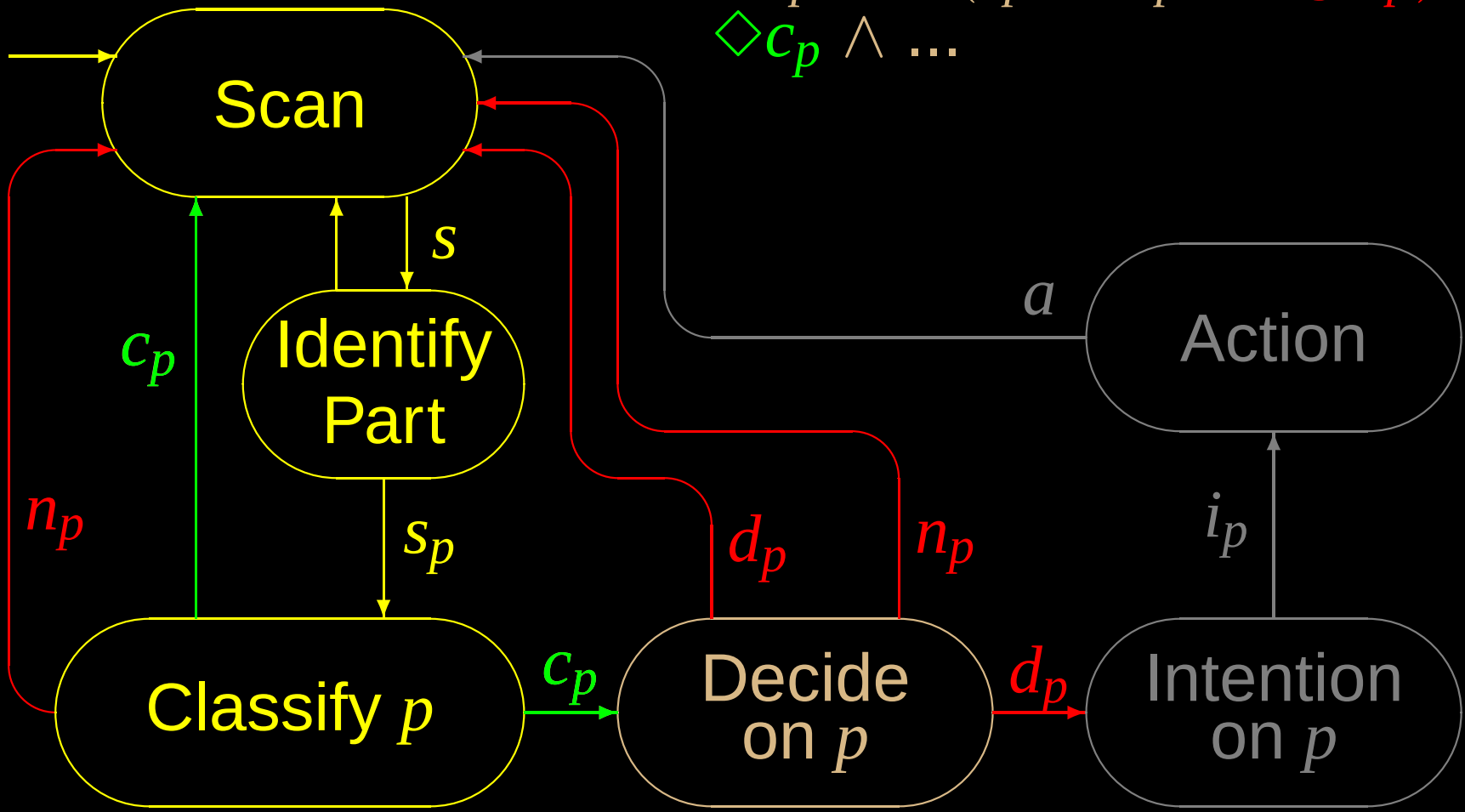
Persistent Mis-prioritisation

no_intended_response$_p$:

$\Box\neg\, s_p$

$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

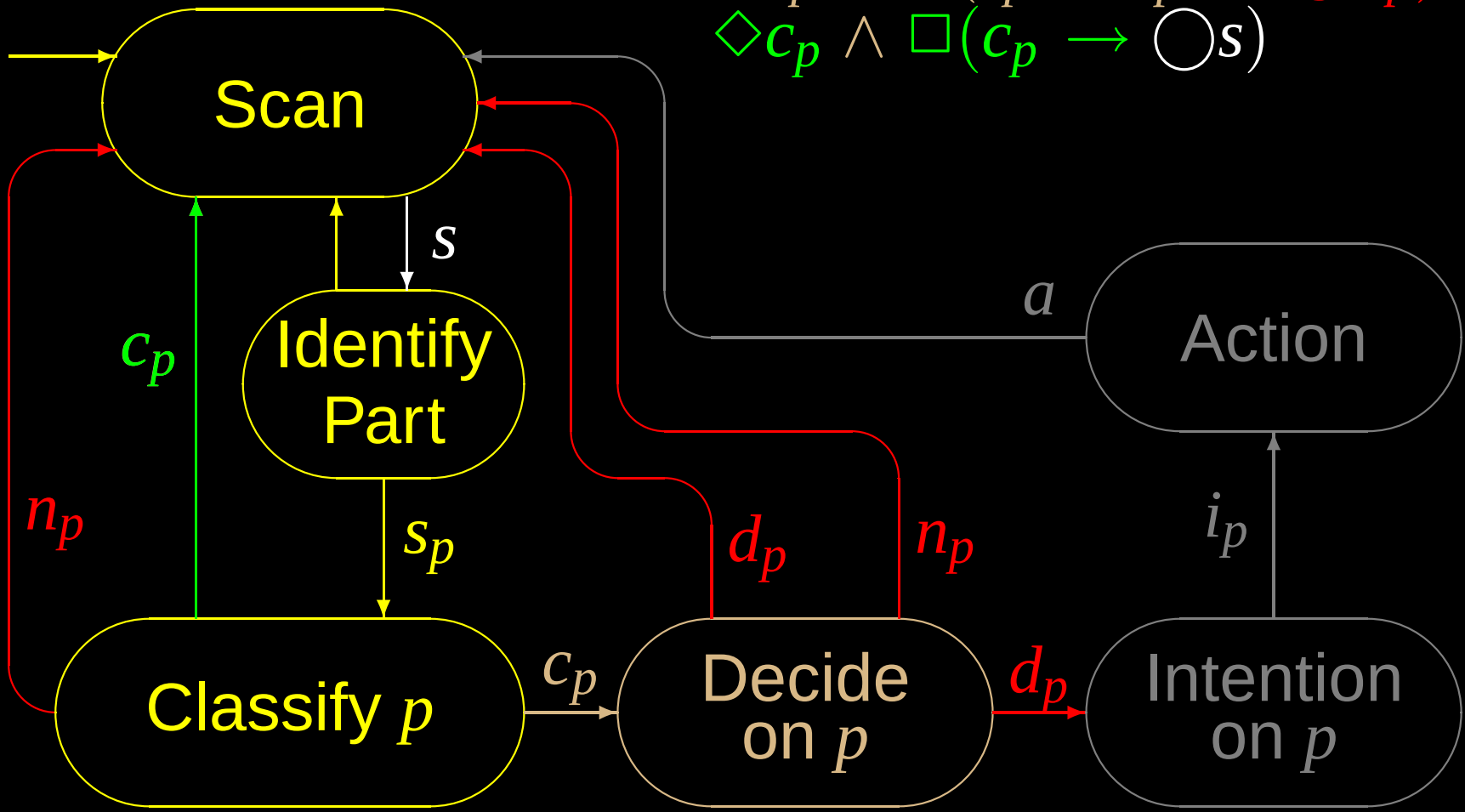
$\Diamond c_p \wedge \ldots$



Persistent Mis-prioritisation

no_intended_response$_p$:

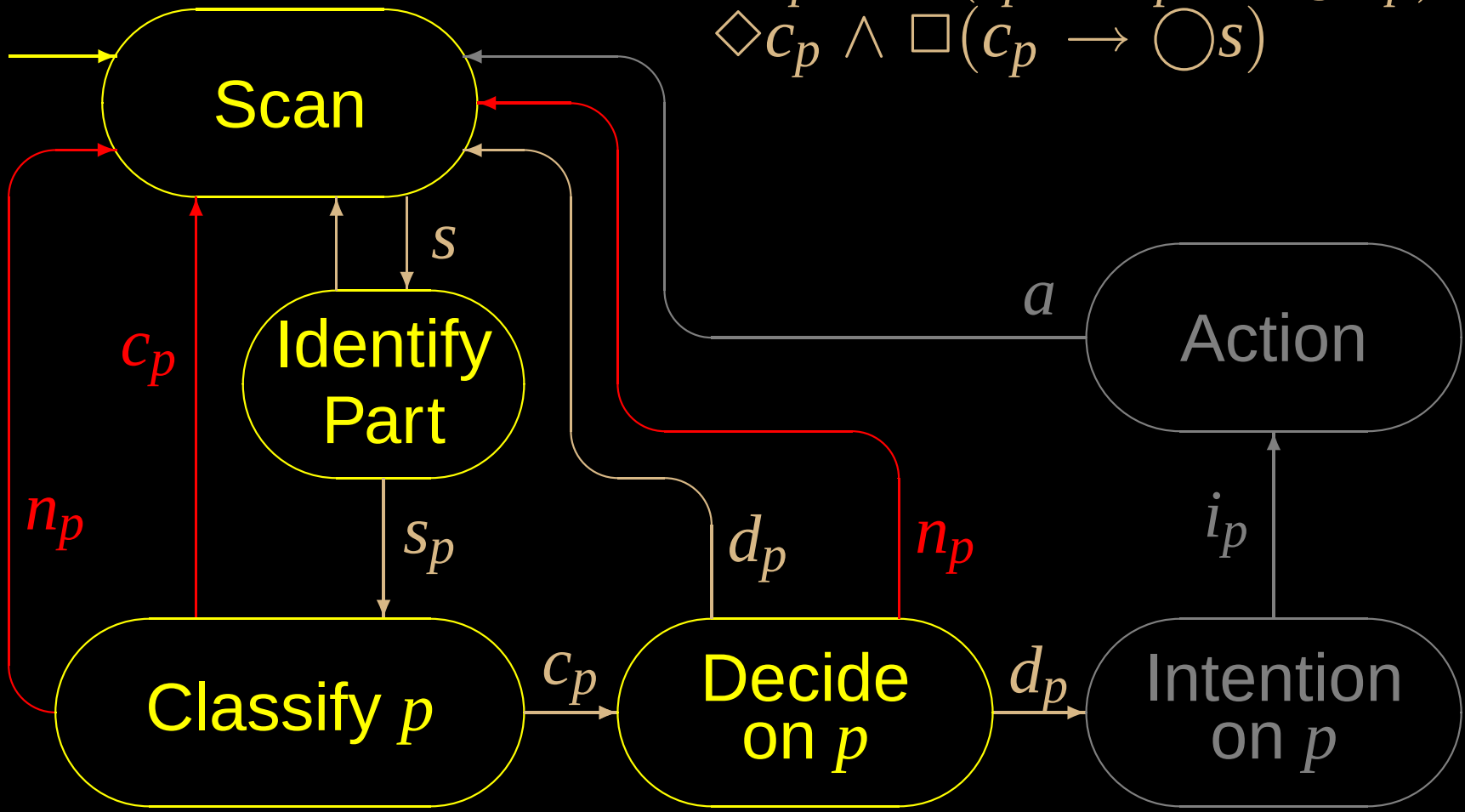
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$



Defer Action for Too Long

no_intended_response$_p$:

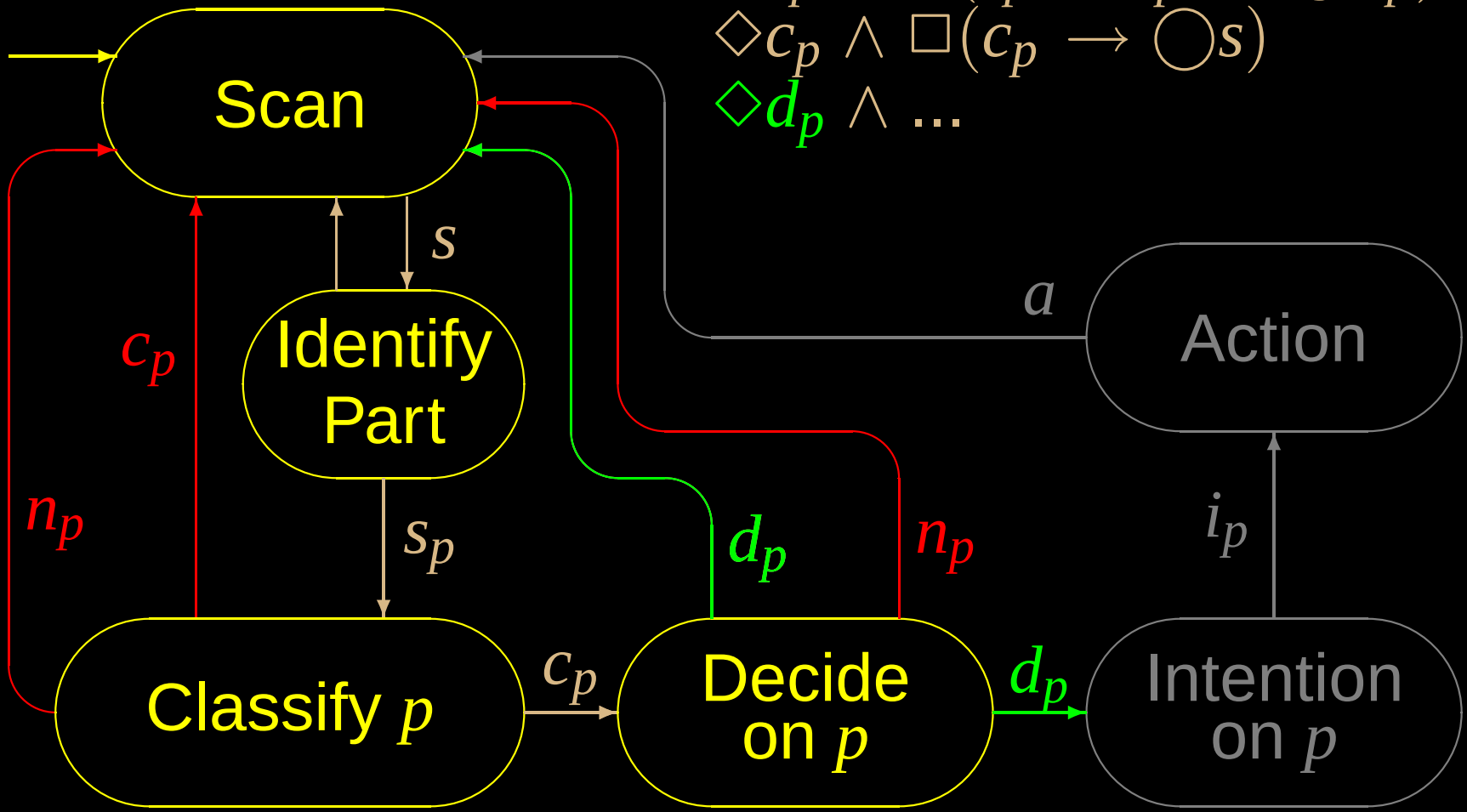
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$



Defer Action for Too Long

$no\_intended\_response_p$:

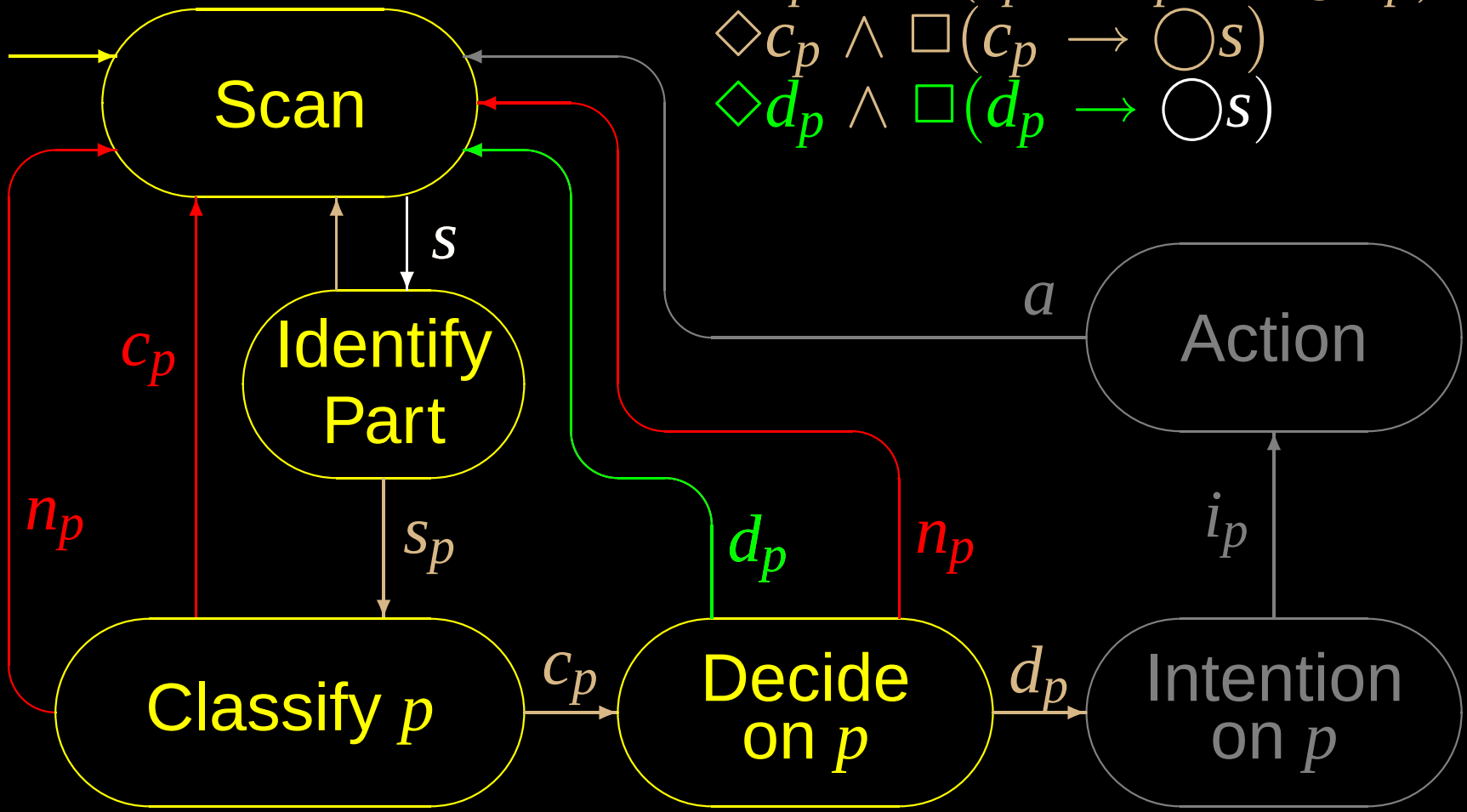
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond d_p \wedge \ldots$$



Defer Action for Too Long

no_intended_response$_p$:

$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$$



Final Decomposition

$$\mathcal{D}\ (\mathit{no\_intended\_response}_p) = \{\Box\neg\ s_p\ ,$$
$$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)\ ,$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)\ ,$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)\ \}$$

Final Decomposition

$$\mathcal{D}\ (\mathit{no\_intended\_response}_p) = \{\Box\neg\ s_p\ ,\ \Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)\ ,\ \Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)\ ,\ \Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)\ \}$$

$$\begin{aligned}
&\mathcal{D}\ (\mathit{non_response}_p)\\
&= \{f \wedge \mathit{non_resolved}_p \mid f \in \mathcal{D}\ (\mathit{no_intended_response}_p)\}\\
&= \{\Box\neg\ s_p \wedge \mathit{non_resolved}_p,\\
&\quad \Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p\ ) \wedge \mathit{non_resolved}_p,\\
&\quad \Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s) \wedge \mathit{non_resolved}_p,\\
&\quad \Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s) \wedge \mathit{non_resolved}_p\}
\end{aligned}$$

Proofs

- Existence of the Task Failures.
- Disjunction of the Task Failures.
- Soundness of the Decomposition.
- Completeness of the Decomposition.

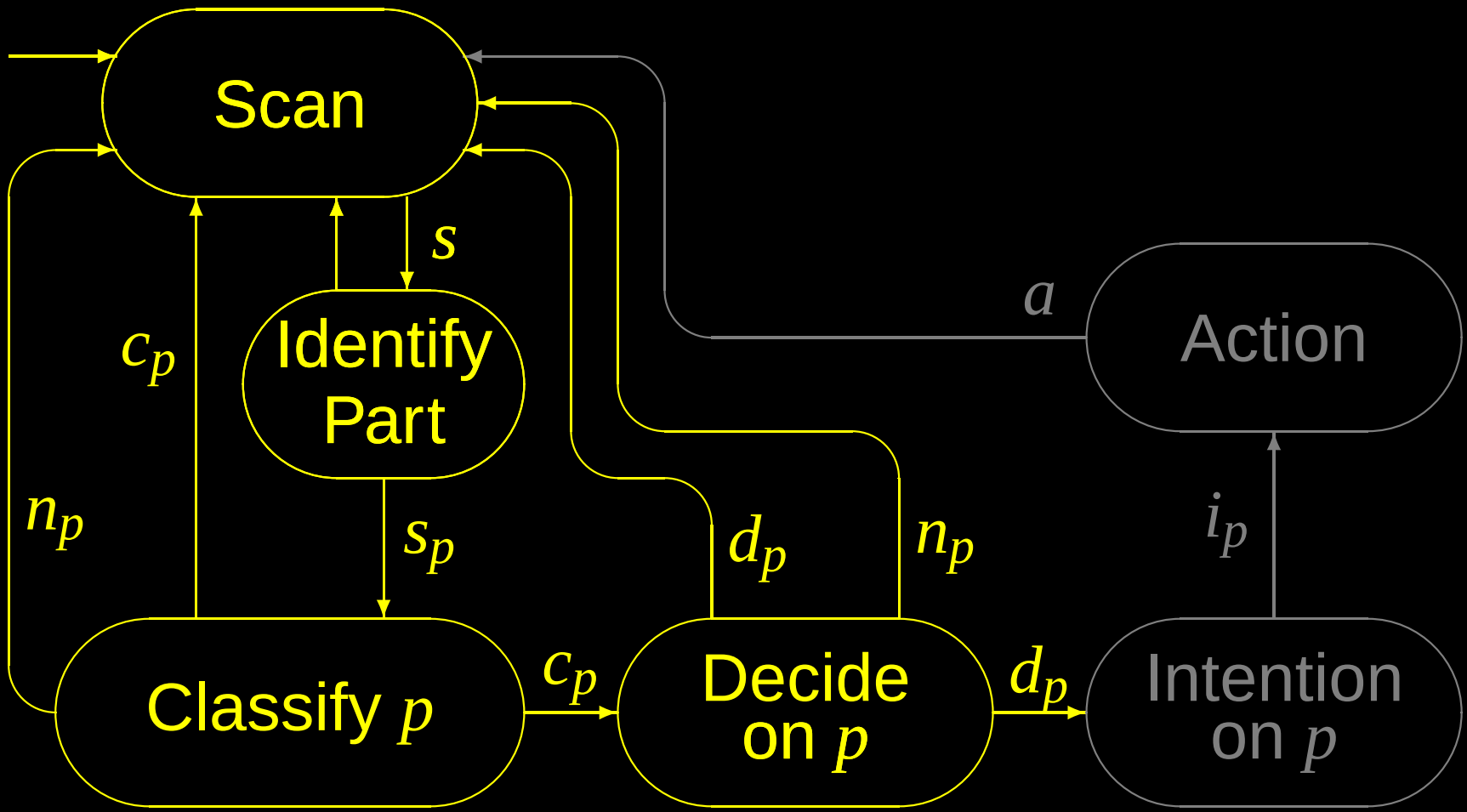
$$OCM \models (\Box \neg\, i_p) \rightarrow \bigvee_{f \in \mathcal{F}} f,$$

where

$$\mathcal{F} = \{fail\_scan_p, pers\_mis\_clas_p, pers\_mis\_prio_p \\ cont\_dec\_proc_p, def\_too\_long_p\}$$

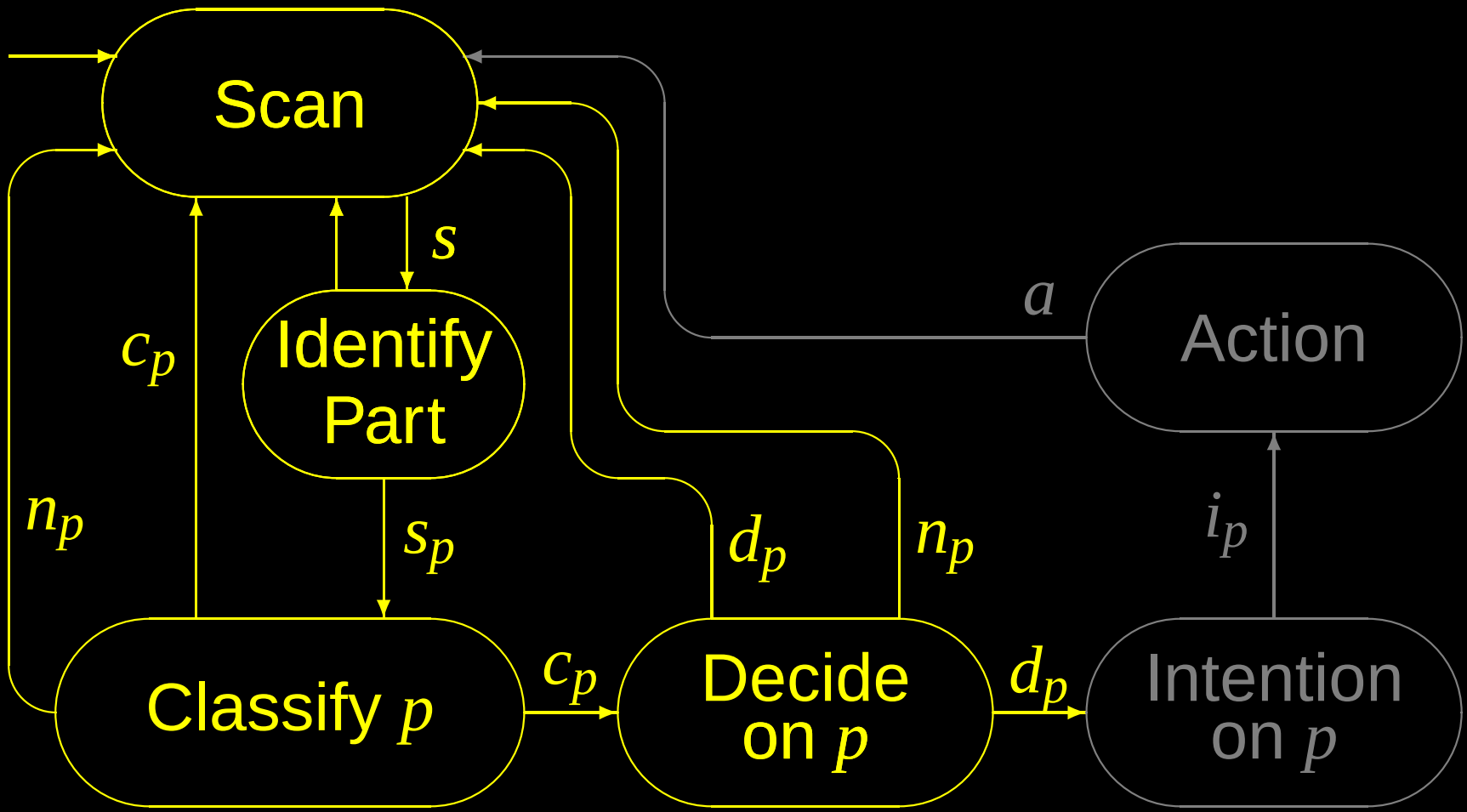
Soundness

Soundness


Scan
Identify Part
Classify p
Decide on p
Action
Intention on p
s
c_p
n_p
s_p
d_p
n_p
a
i_p
c_p
d_p

Soundness

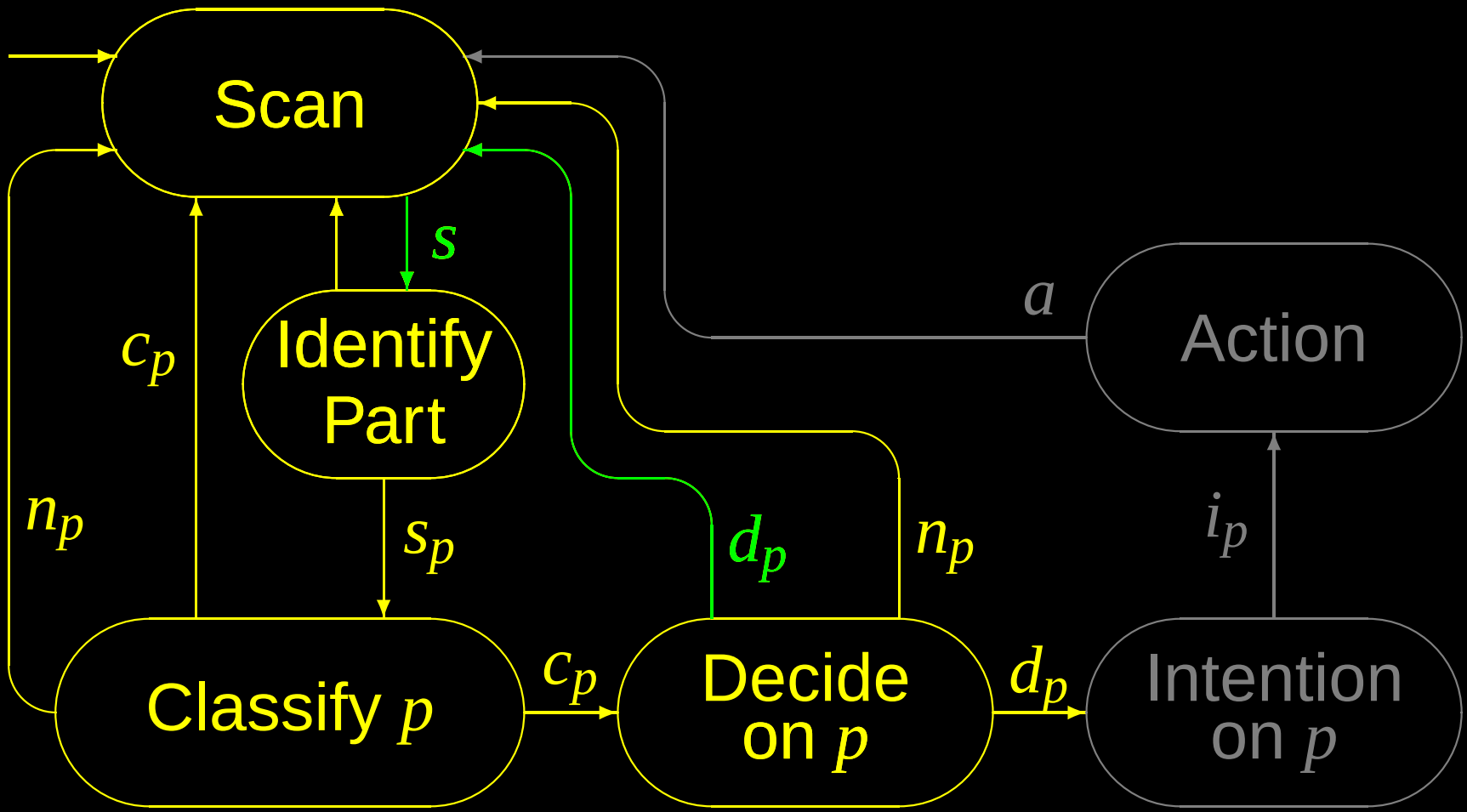
Example: Defer action for too long



Soundness

Example: Defer action for too long

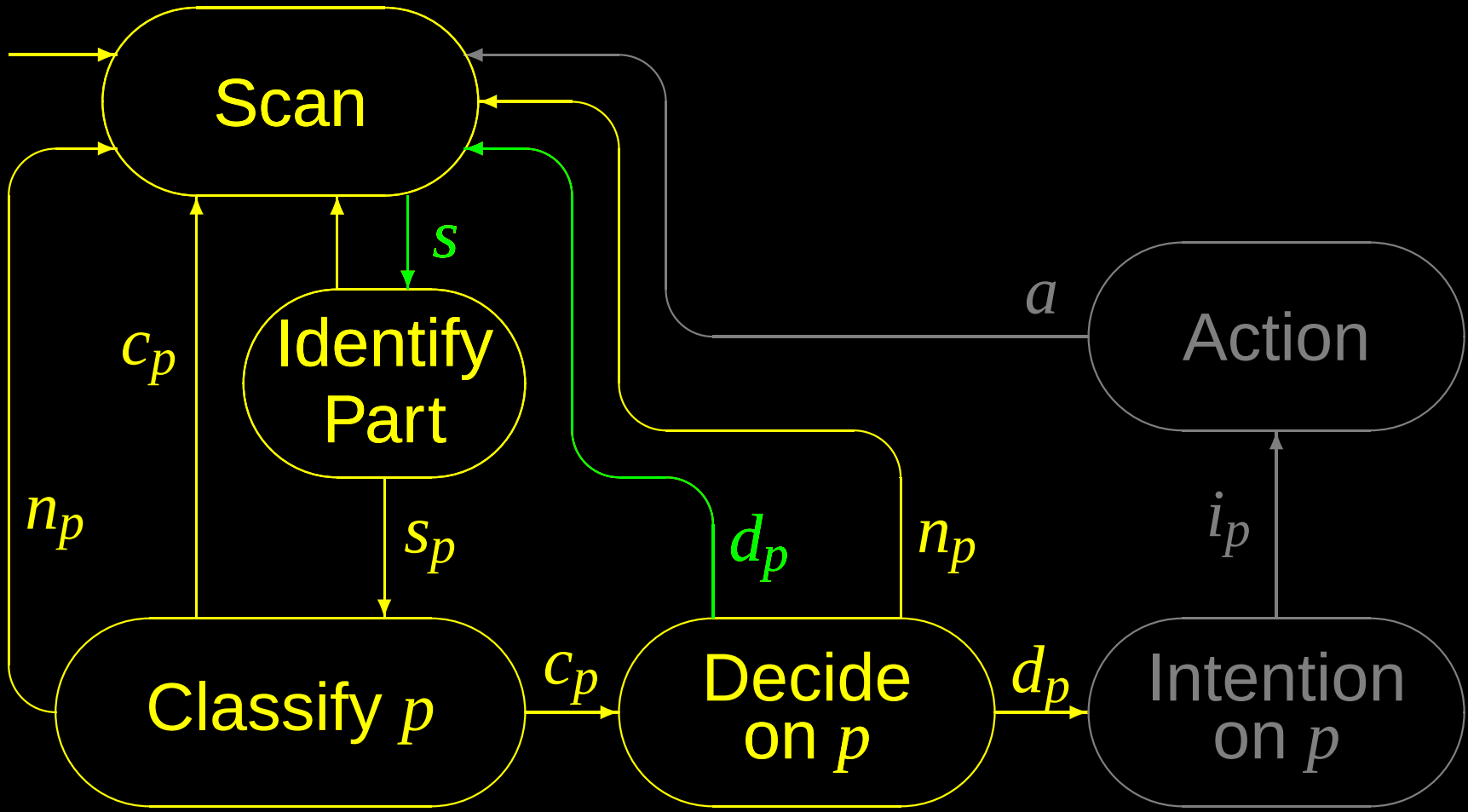
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$$



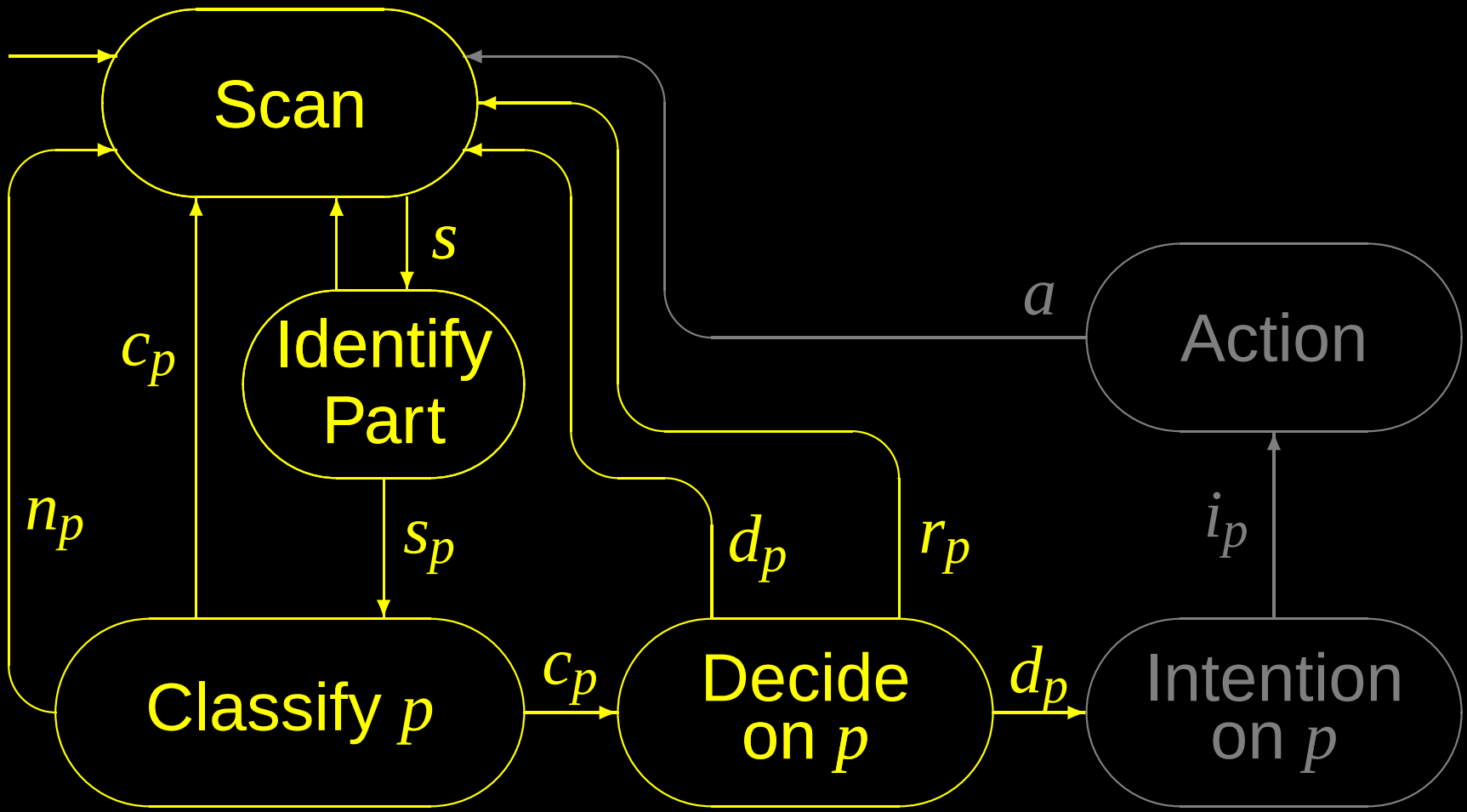
Soundness

Example: Defer action for too long

$$(\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)) \rightarrow \Box\neg\, i_p$$

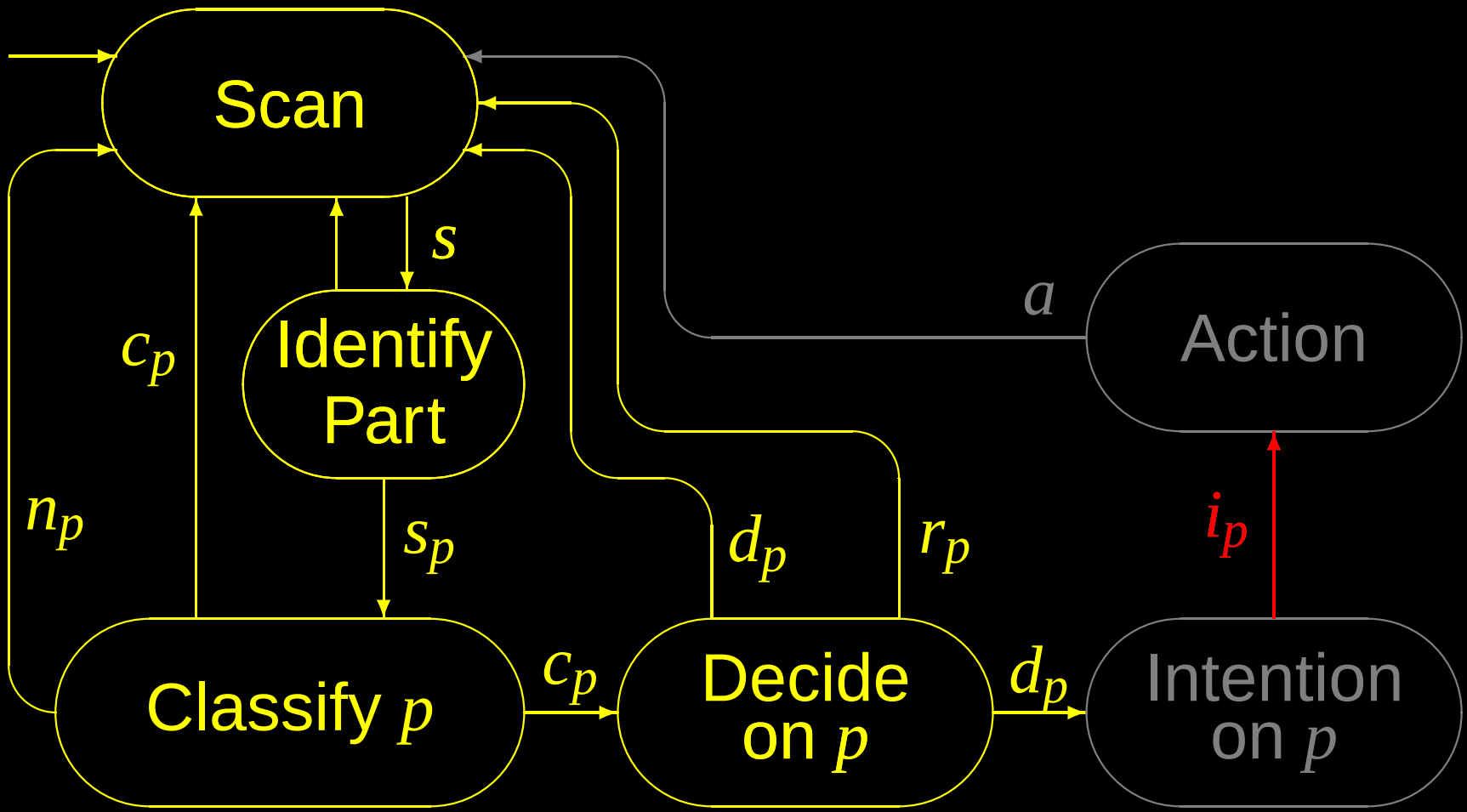


Completeness



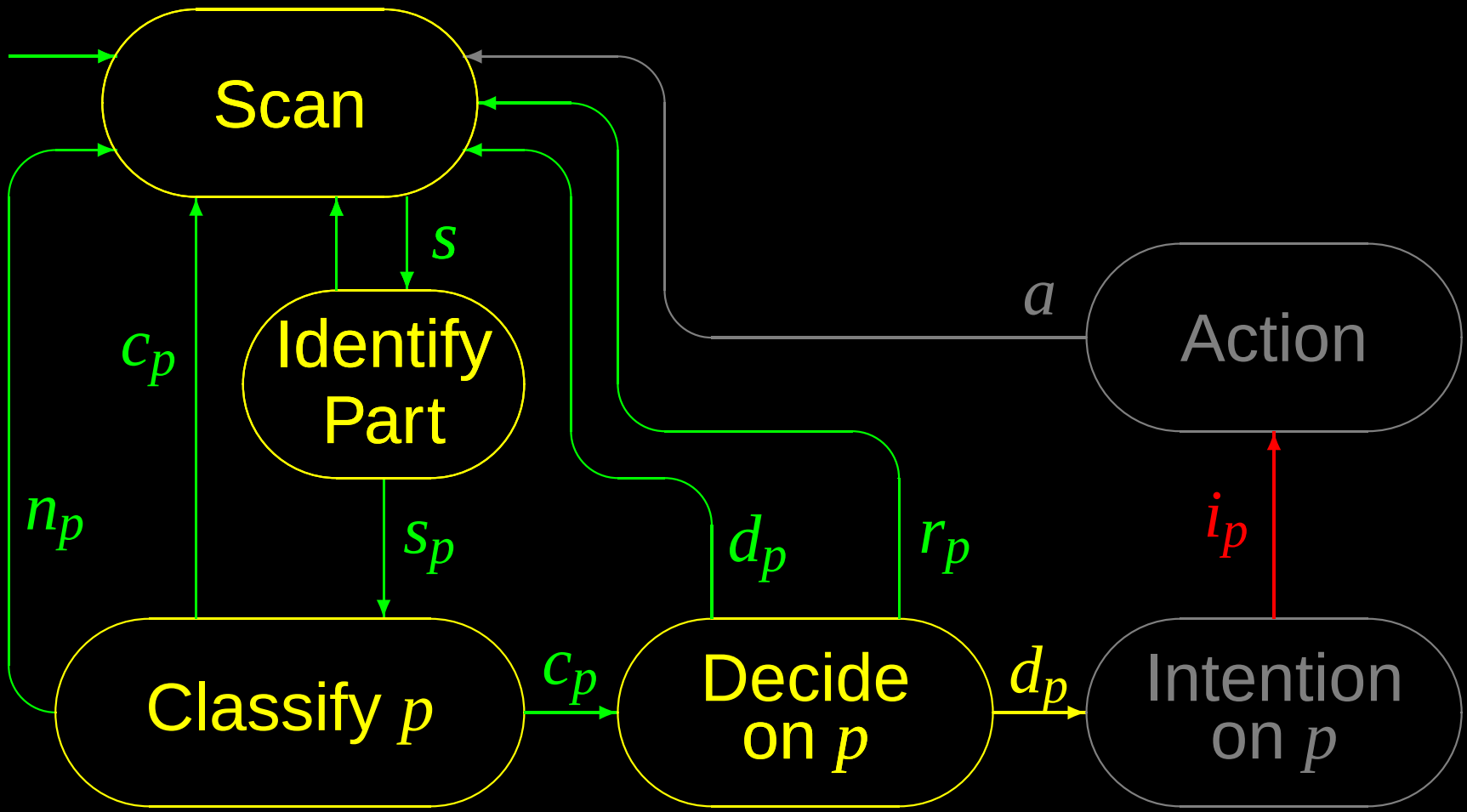
Completeness

$\Box\neg\, i_p \ \ldots$



Completeness

$\Box\neg\, i_p \rightarrow \ldots$



Completeness

$$\Box\neg\, i_p \;\rightarrow \bigvee_{f\in\mathcal{F}} f$$

where

$$\mathcal{F} \;= \mathcal{D}\;(\Box\neg\, i_p) = \mathcal{D}\;(no\_intended\_response_p) =$$

Completeness

$$\Box\neg\, i_p \;\rightarrow \bigvee_{f\in\mathcal{F}} f$$

where

$$\mathcal{F} \;= \mathcal{D}\;(\Box\neg\, i_p) = \mathcal{D}\;(no\_intended\_response_p) =$$
$$\{\, \Box\neg\, s_p\;,$$
$$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)\;,$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)\;,$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)\;\}$$

Model-checking Properties

using The Concurrency Workbench of the New Century

http://www.cs.sunysb.edu/∼cwb/

Model-checking Properties

using The Concurrency Workbench of the New Century
http://www.cs.sunysb.edu/∼cwb/

- Soundness $\Longrightarrow$ YES

Model-checking Properties

using The Concurrency Workbench of the New Century
http://www.cs.sunysb.edu/∼cwb/

- Soundness $\Longrightarrow$ YES
- Completeness $\Longrightarrow$ NO

Model-checking Properties

using The Concurrency Workbench of the New Century
http://www.cs.sunysb.edu/∼cwb/

- Soundness $\Longrightarrow$ YES
- Completeness $\Longrightarrow$ NO
  $\Longrightarrow$ counterexample

Exercise

Exercise

- Which error did I (deliberately) make while explaining the decomposition?

Exercise

- Which error did I (deliberately) make while explaining the decomposition?
- What caused such an error?

Exercise

- Which error did I (deliberately) make while explaining the decomposition?
- What caused such an error?
- Find and analyse the counterexample which falsifies completeness

Exercise

- Which error did I (deliberately) make while explaining the decomposition?
- What caused such an error?
- Find and analyse the counterexample which falsifies completeness
- Does the model need to be modified?

Exercise

- Which error did I (deliberately) make while explaining the decomposition?
- What caused such an error?
- Find and analyse the counterexample which falsifies completeness
- Does the model need to be modified?
- Does the decomposition need to be modified?

Exercise

- Which error did I (deliberately) make while explaining the decomposition?
- What caused such an error?
- Find and analyse the counterexample which falsifies completeness
- Does the model need to be modified?
- Does the decomposition need to be modified?
- Modify model and/or decomposition to achieve completeness

Exercise

- Which error did I (deliberately) make while explaining the decomposition?
- What caused such an error?
- Find and analyse the counterexample which falsifies completeness
- Does the model need to be modified?
- Does the decomposition need to be modified?
- Modify model and/or decomposition to achieve completeness
- Give a psychological interpretation to the task failure in the correct decomposition

Any Solution?

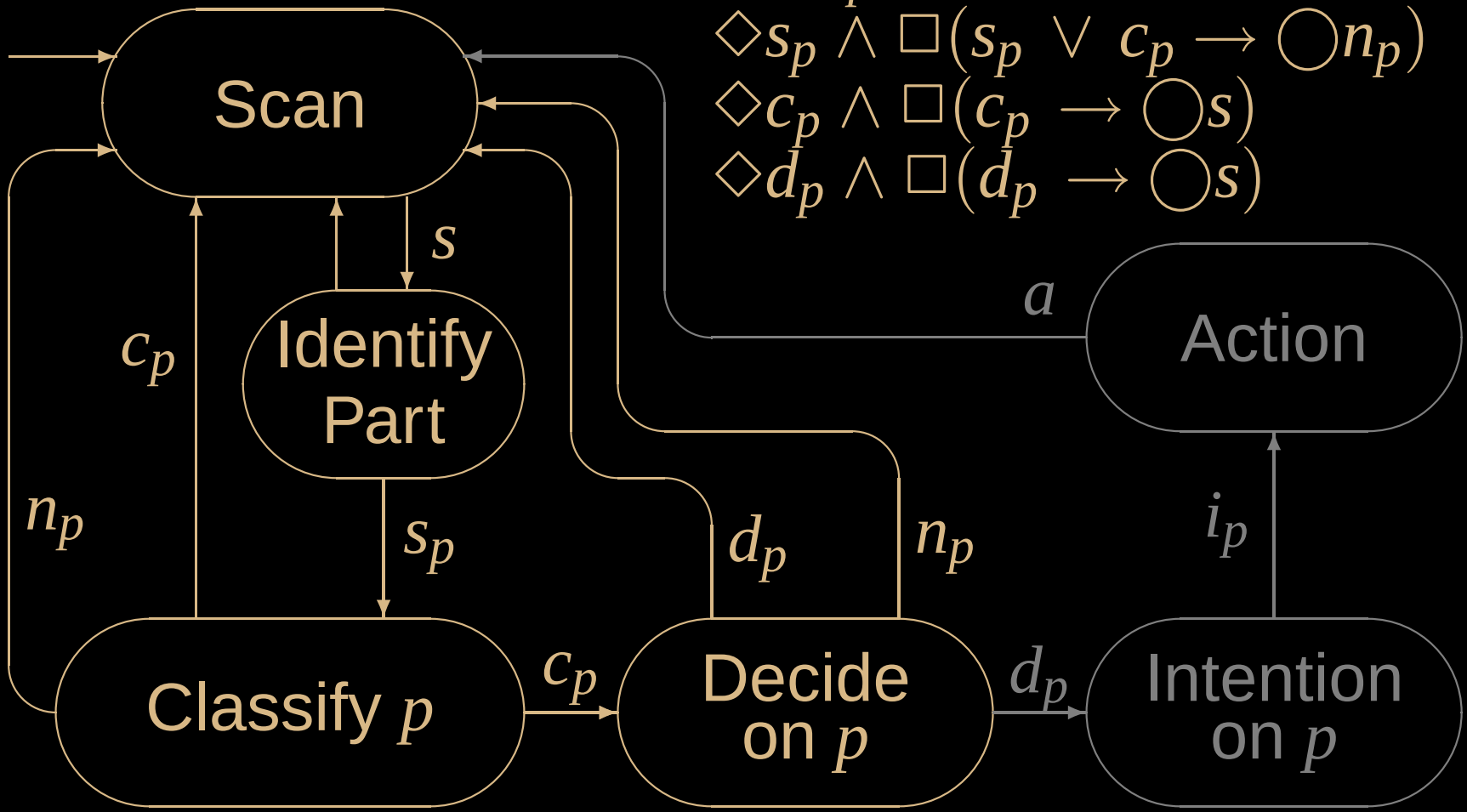
$no\_intended\_response_p$:

$\Box \neg s_p$

$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$

$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$

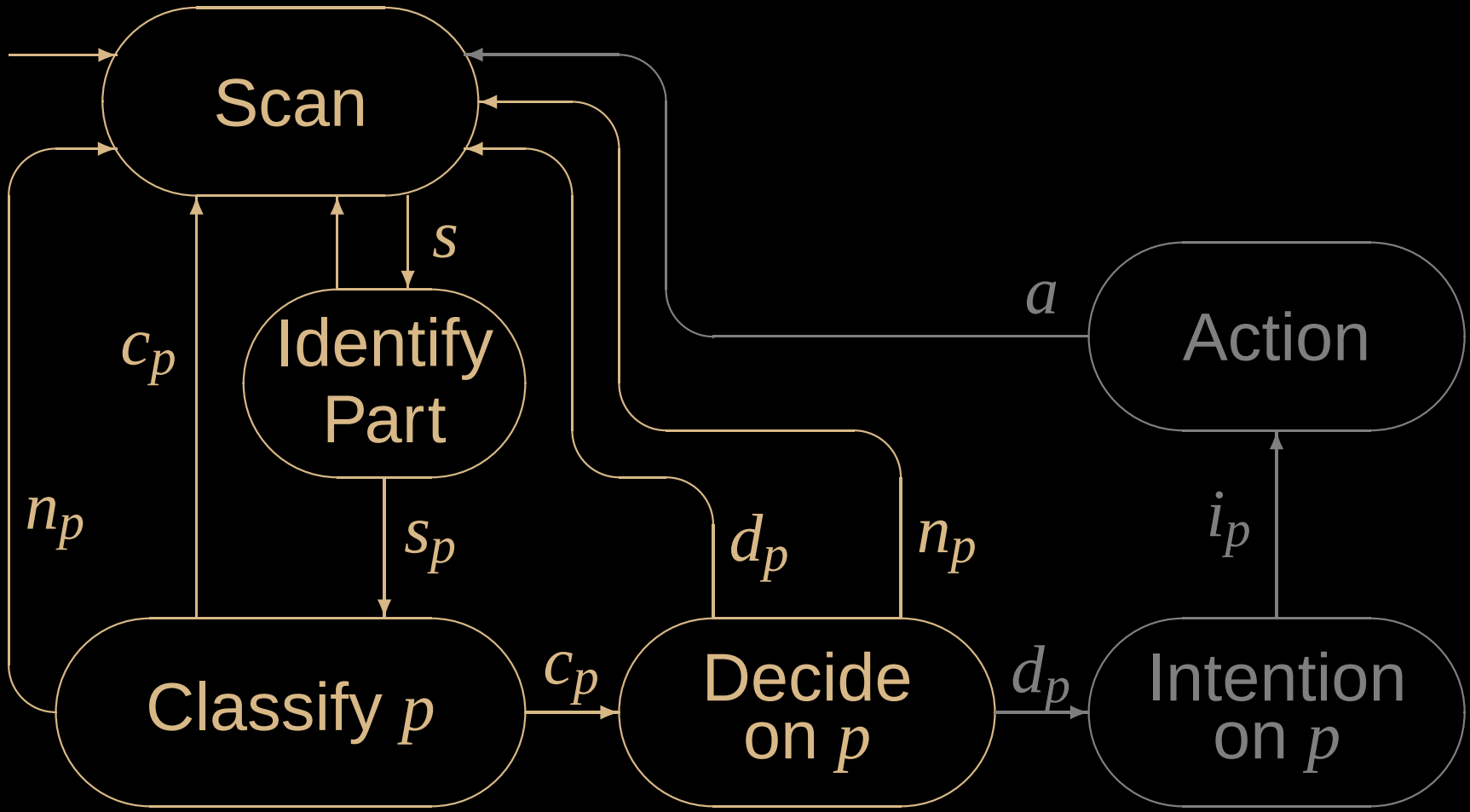


Solution: Counterexample

Find and analyse the counterexample which falsifies completeness

Solution: Counterexample

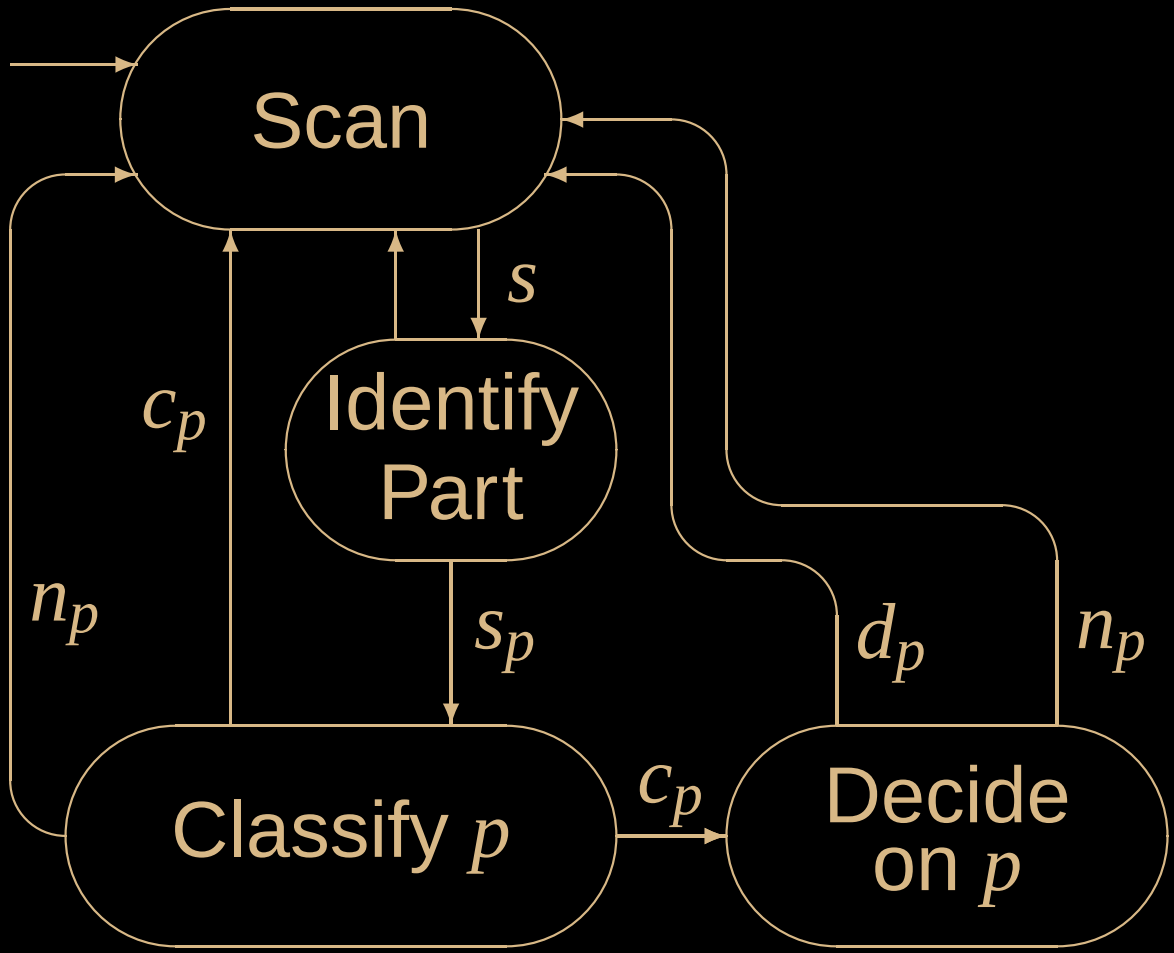
Find and analyse the counterexample



Solution: Counterexample

Find and analyse the counterexample

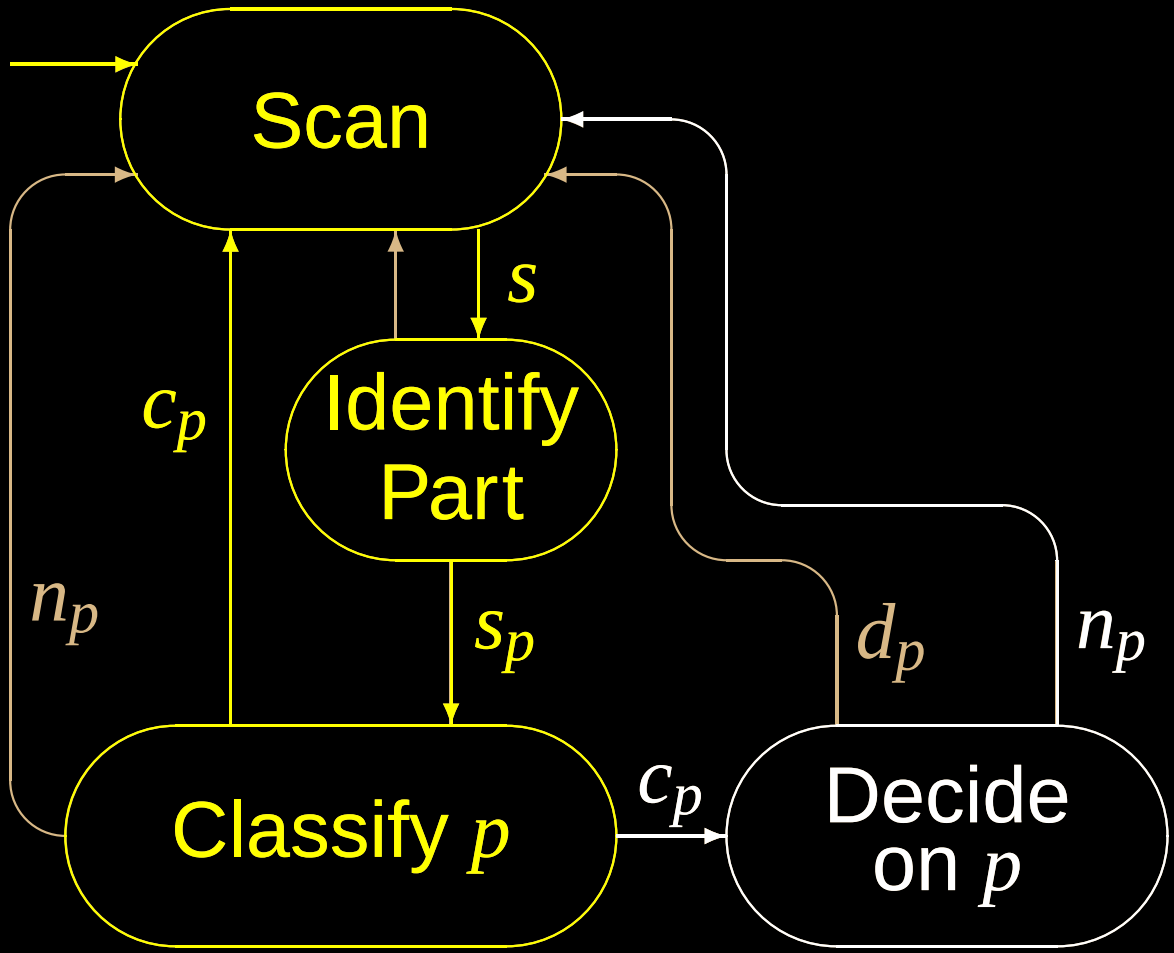
$$s \longrightarrow s_p \longrightarrow c_p \longrightarrow s \longrightarrow s_p \longrightarrow c_p \longrightarrow n_p \longrightarrow s \longrightarrow \ldots$$



Solution: Counterexample

Find and analyse the counterexample

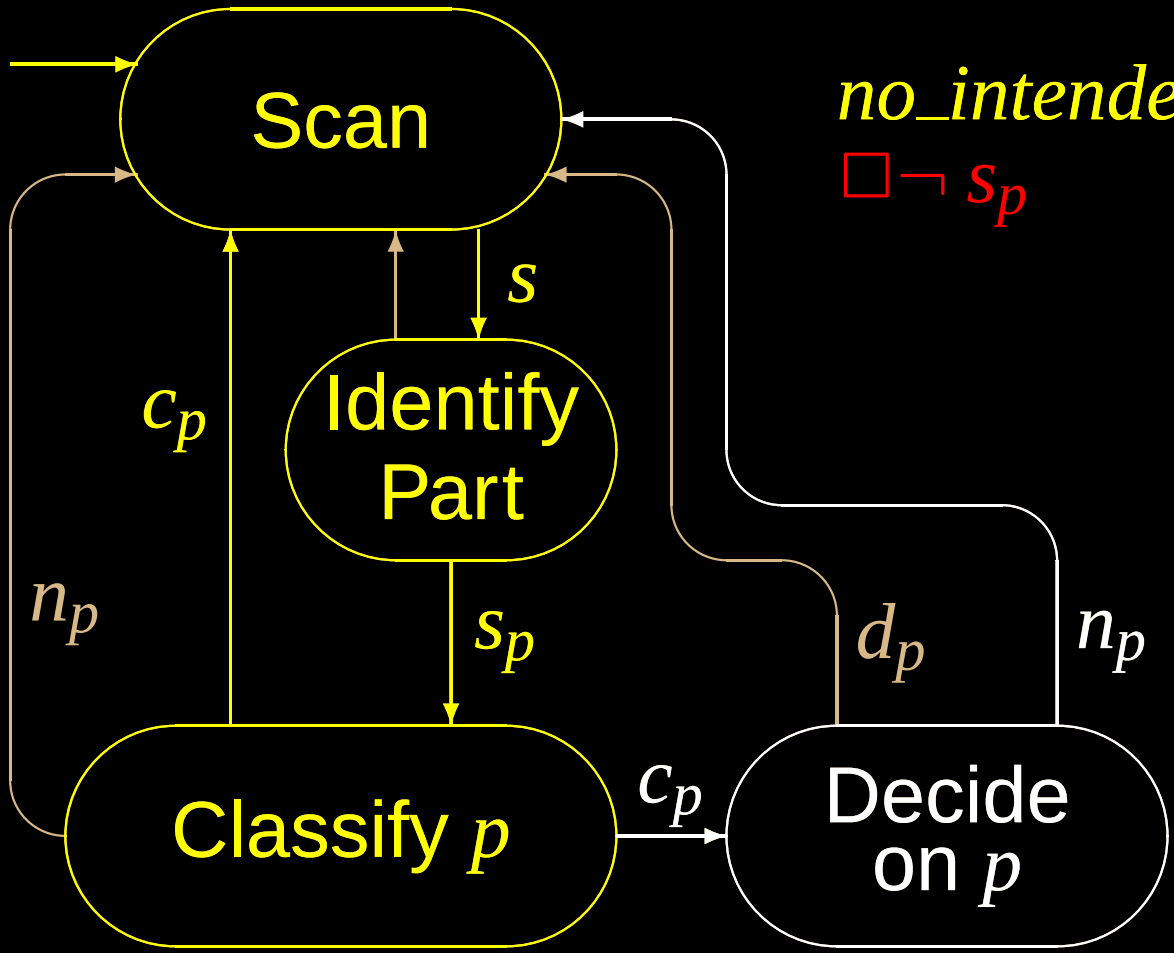
$$s \longrightarrow s_p \longrightarrow c_p \longrightarrow s \longrightarrow s_p \longrightarrow c_p \longrightarrow n_p \longrightarrow s \longrightarrow \ldots$$



Solution: Counterexample

Find and analyse the counterexample

$s \longrightarrow s_p \longrightarrow c_p \longrightarrow s \longrightarrow s_p \longrightarrow c_p \longrightarrow n_p \longrightarrow s \longrightarrow \ldots$



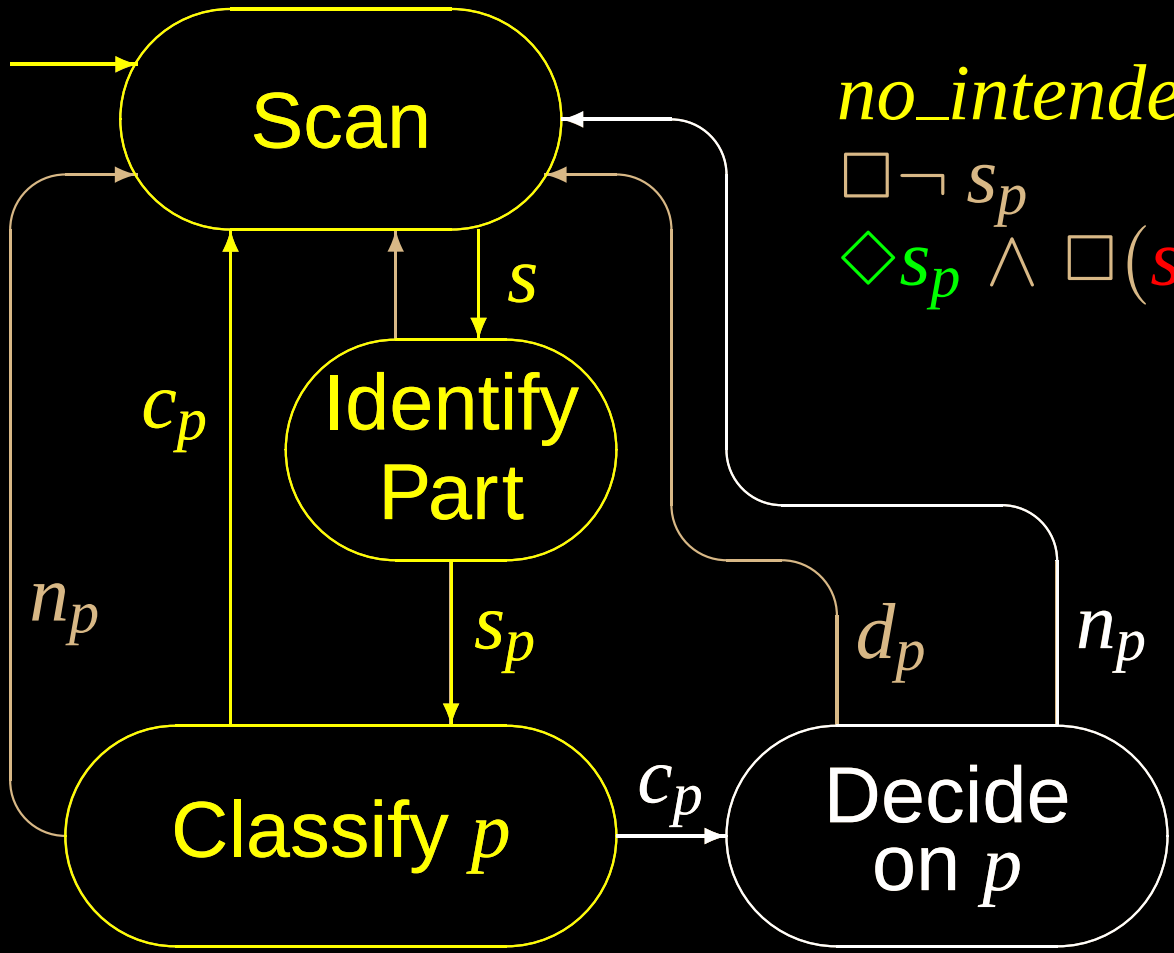
$no\_intended\_response_p$:

$\Box \neg s_p$

Solution: Counterexample

Find and analyse the counterexample

$s \longrightarrow s_p \longrightarrow c_p \longrightarrow s \longrightarrow s_p \longrightarrow c_p \longrightarrow n_p \longrightarrow s \longrightarrow \ldots$



$no\_intended\_response_p$:

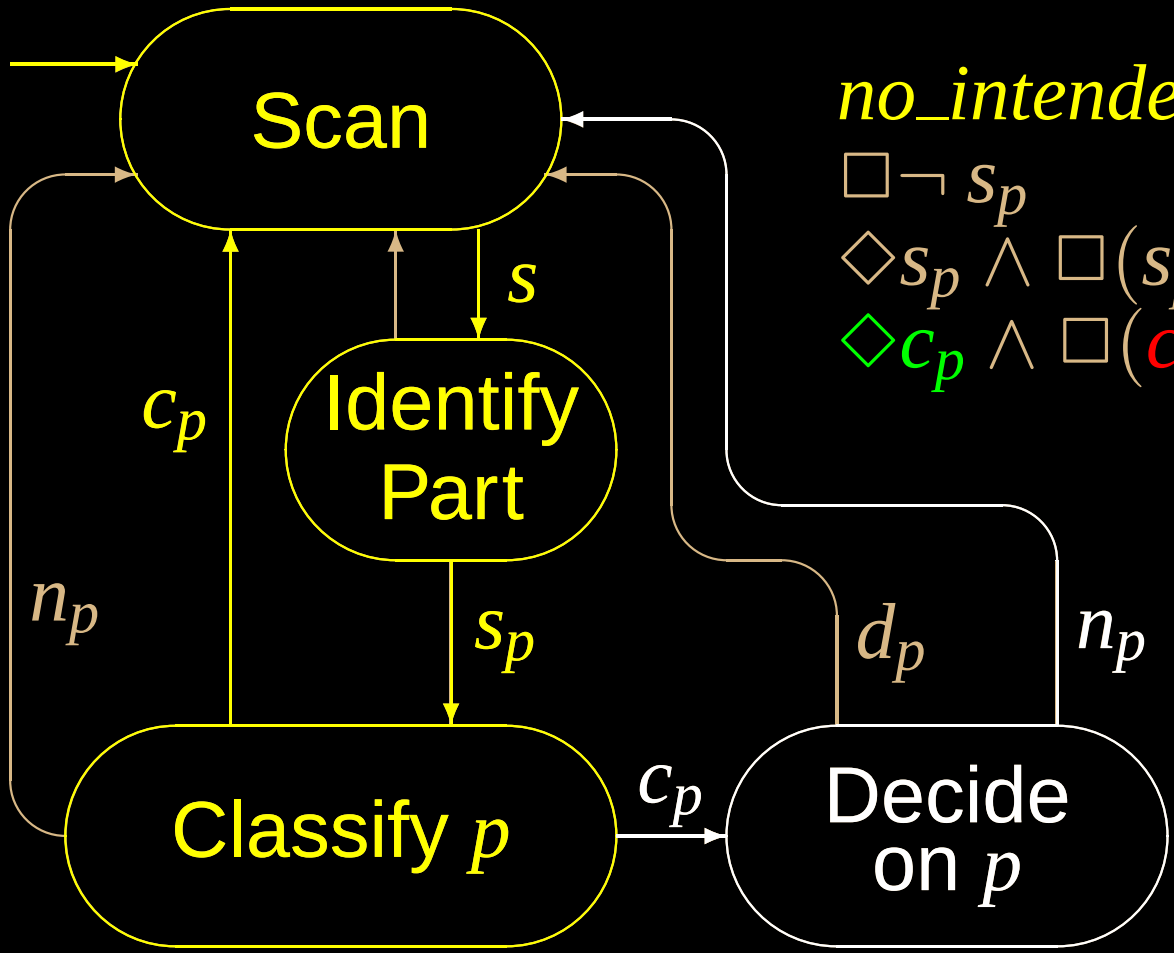
$\Box \neg s_p$

$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

Solution: Counterexample

Find and analyse the counterexample

$$s \longrightarrow s_p \longrightarrow c_p \longrightarrow s \longrightarrow s_p \longrightarrow c_p \longrightarrow n_p \longrightarrow s \longrightarrow \ldots$$



$no\_intended\_response_p$:

$\Box\neg\, s_p$

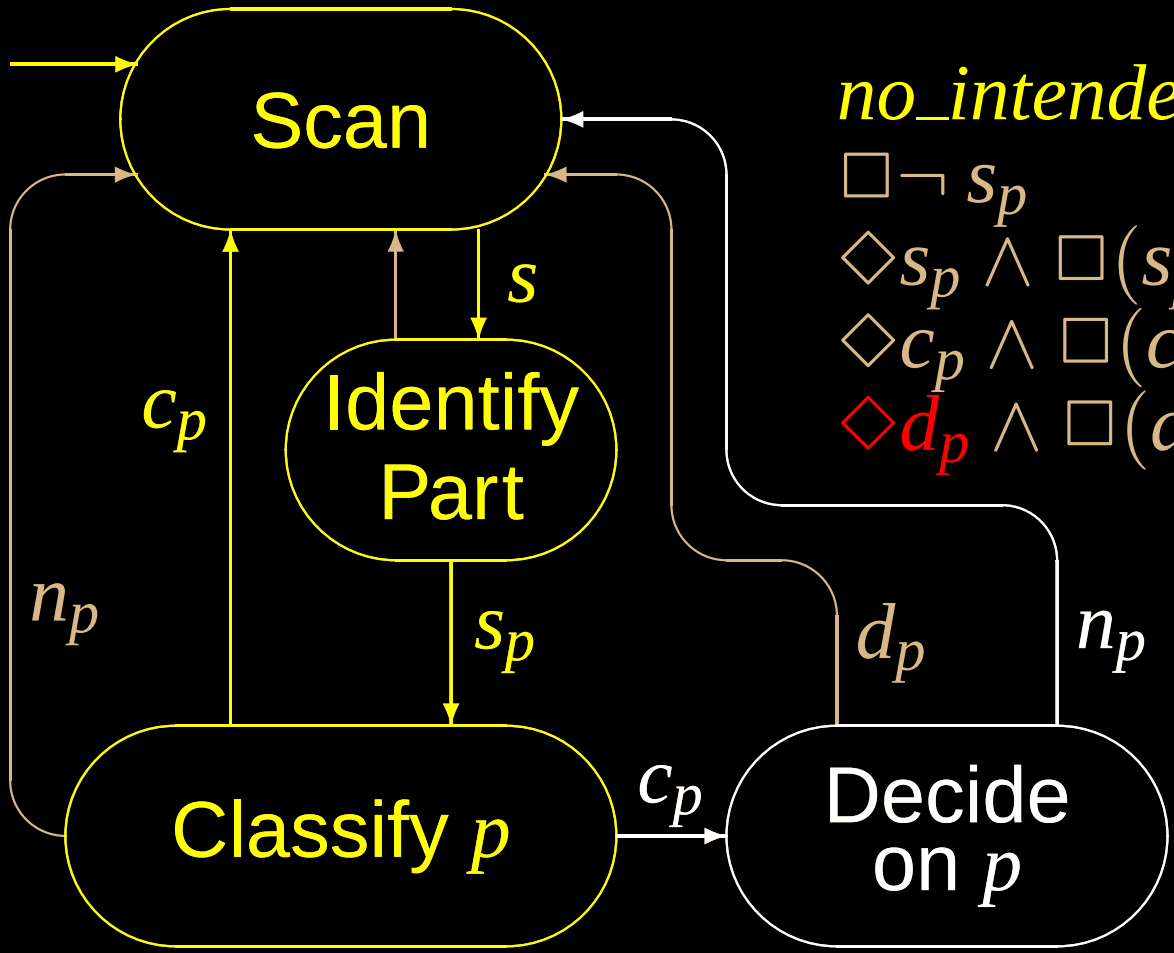
$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$

Solution: Counterexample

Find and analyse the counterexample

$$s \longrightarrow s_p \longrightarrow c_p \longrightarrow s \longrightarrow s_p \longrightarrow c_p \longrightarrow n_p \longrightarrow s \longrightarrow \ldots$$



$no\_intended\_response_p$:

$\Box\neg\, s_p$

$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

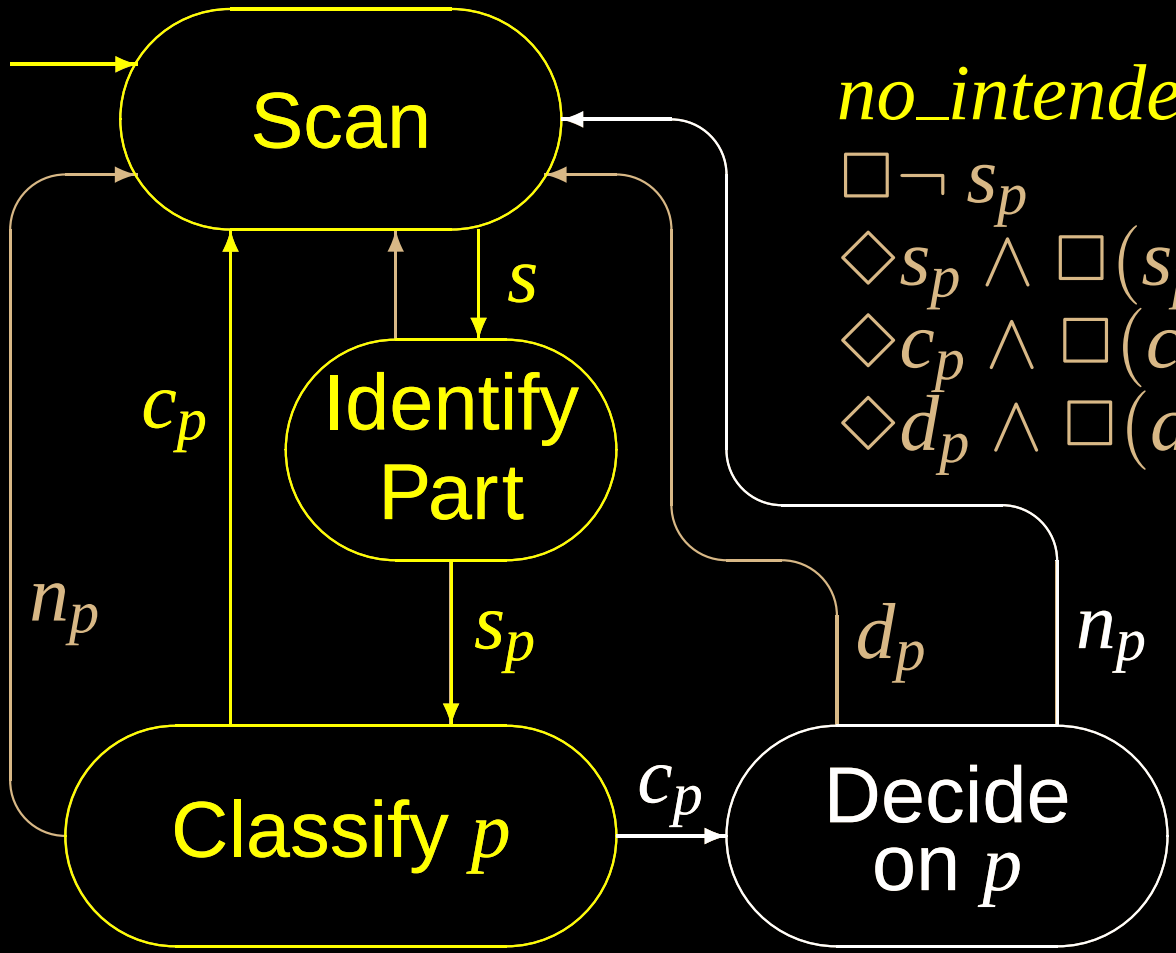
$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$

$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$

Solution: Counterexample

Find and analyse the counterexample

$$s \longrightarrow s_p \longrightarrow c_p \longrightarrow s \longrightarrow s_p \longrightarrow c_p \longrightarrow n_p \longrightarrow s \longrightarrow \ldots$$



$no\_intended\_response_p$:

$\Box\neg\, s_p$

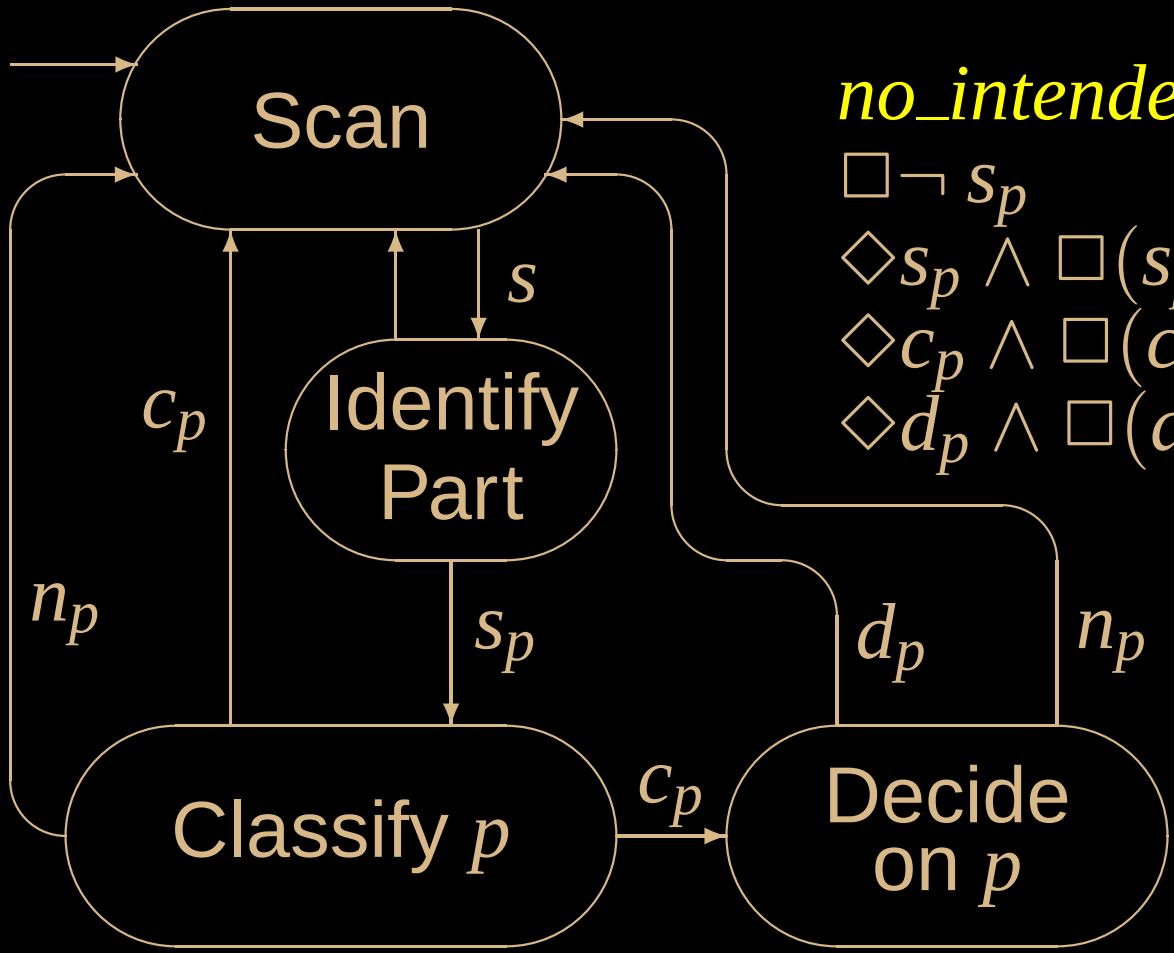
$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$

$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$

Solution: Error

Which error did I (deliberately) make while explaining the decomposition?



$no\_intended\_response_p$:

$\Box\neg\, s_p$

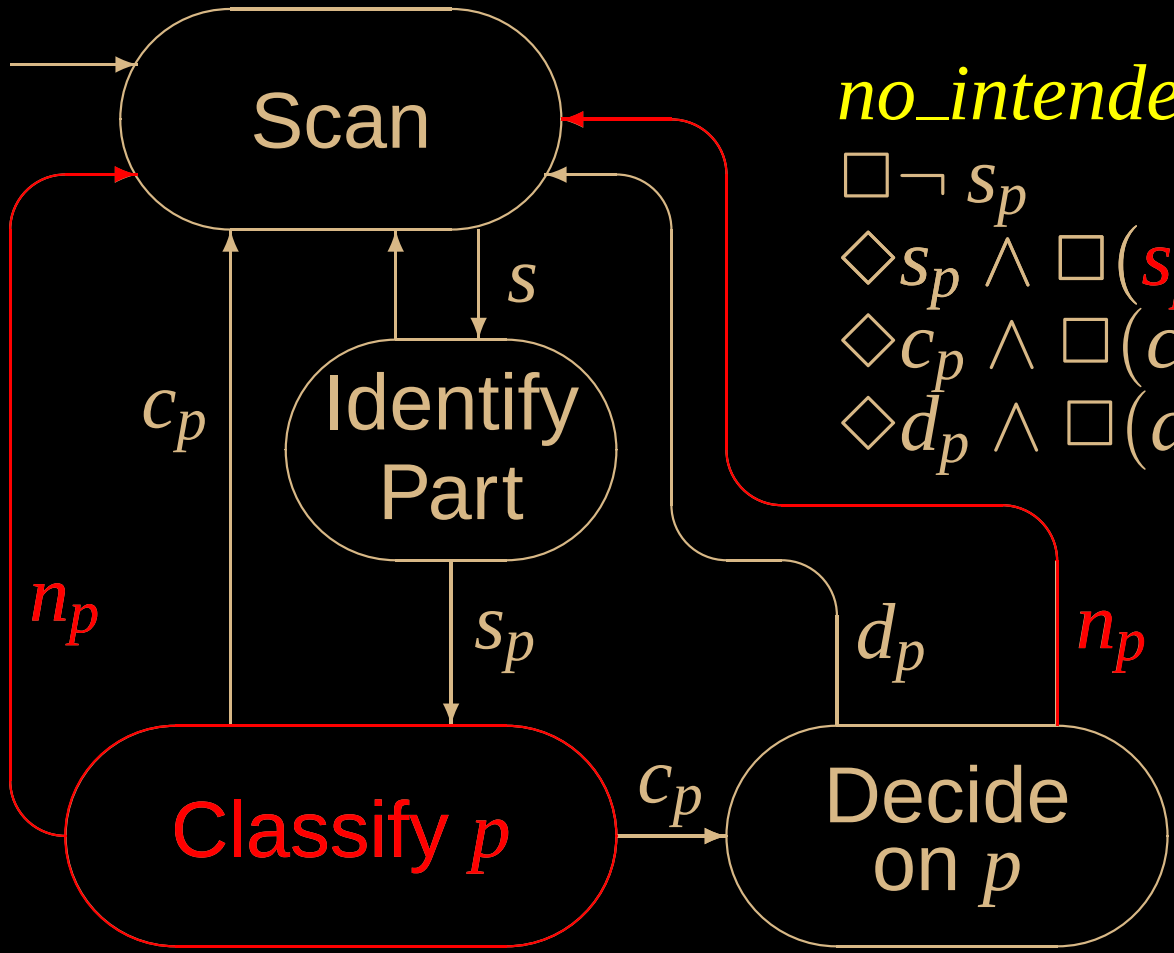
$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$

$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$

Solution: Error

Persisten Mis-classification $\Longleftarrow$ repeated classification as a non conflict causes a perception distorted by the mistaken belief that p is not in conflict



$no\_intended\_response_p$:

$\Box \neg s_p$

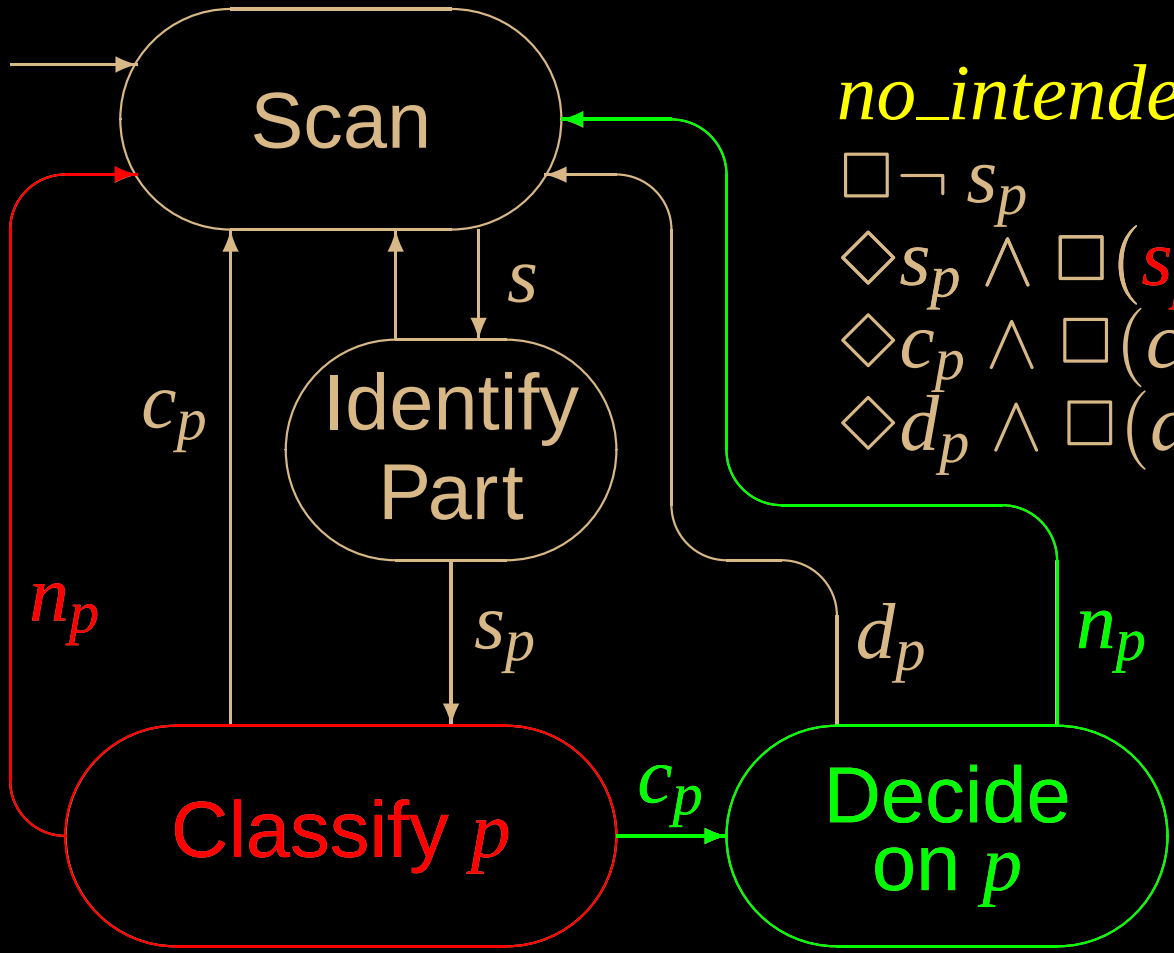
$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$

$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$

Solution: Error

Persisten Mis-classification $\Longleftarrow$ repeated classification as a non conflict causes a perception distorted by the mistaken belief that p is not in conflict



$no\_intended\_response_p$:

$\Box\neg\, s_p$

$\Diamond s_p \wedge \Box(s_p \vee c_p \rightarrow \bigcirc n_p)$

$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$

$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$

Contrary Decision Process $\Longleftarrow$ previous decisions on similar pairs

Solution: Error Cause

What caused such an error?

Solution: Error Cause

What caused such an error?

- use of the same action name n to denote the results of two cognitive processes

Solution: Error Cause

What caused such an error?

- use of the same action name n to denote the results of two cognitive processes
- aim at an elegant and easy to understand (to psychologists) formal model

Solution: Error Cause

What caused such an error?

- use of the same action name n to denote the results of two cognitive processes
- aim at an elegant and easy to understand (to psychologists) formal model
  $\Longrightarrow$ focus on syntactical look of formulae
  rather than on their interpretation on the model

Solution: Model?

Does the model need to be modified?

Solution: Model?

Does the model need to be modified?

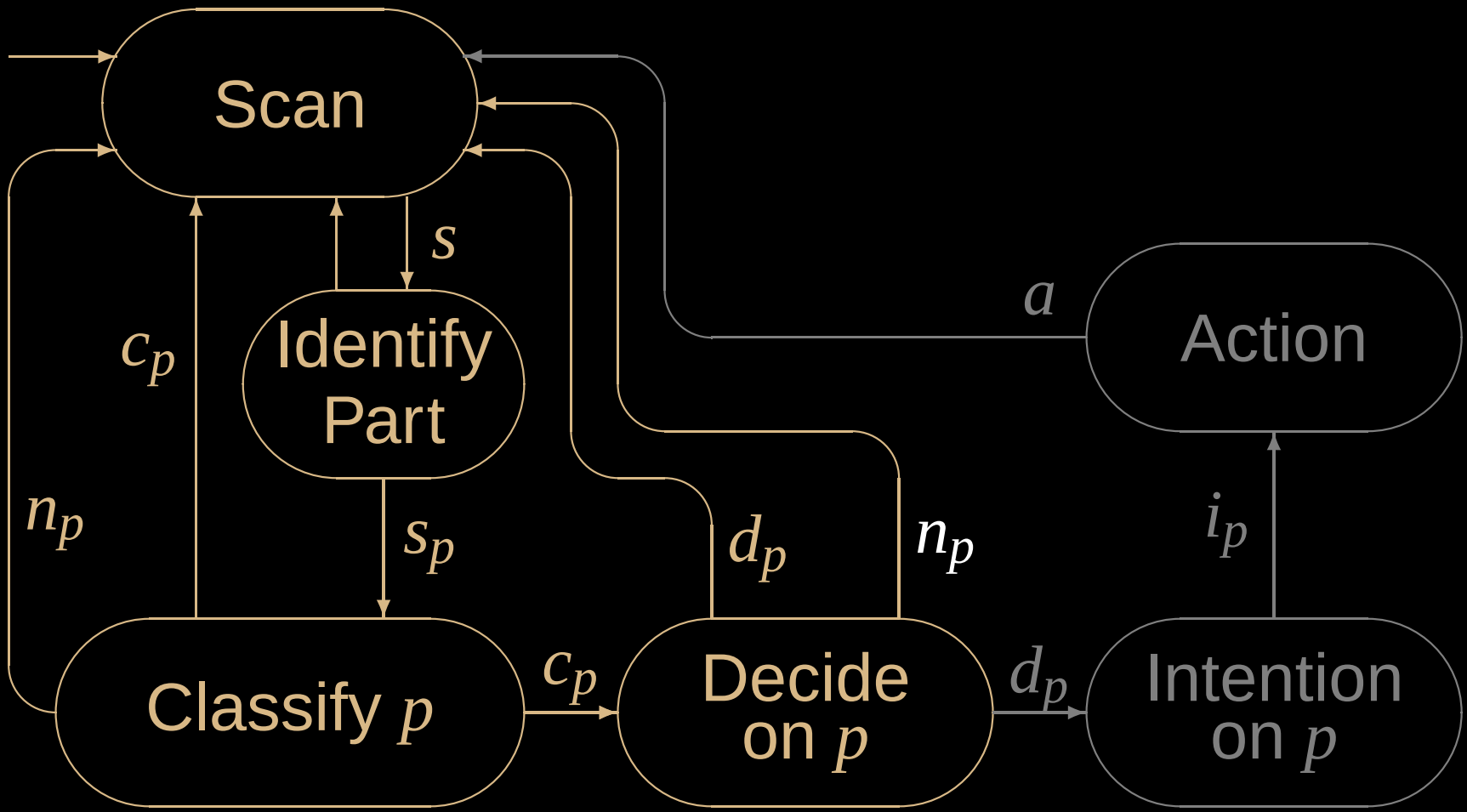
- Error Cause: use of the same action name n to denote the results of two cognitive processes

Solution: Model?

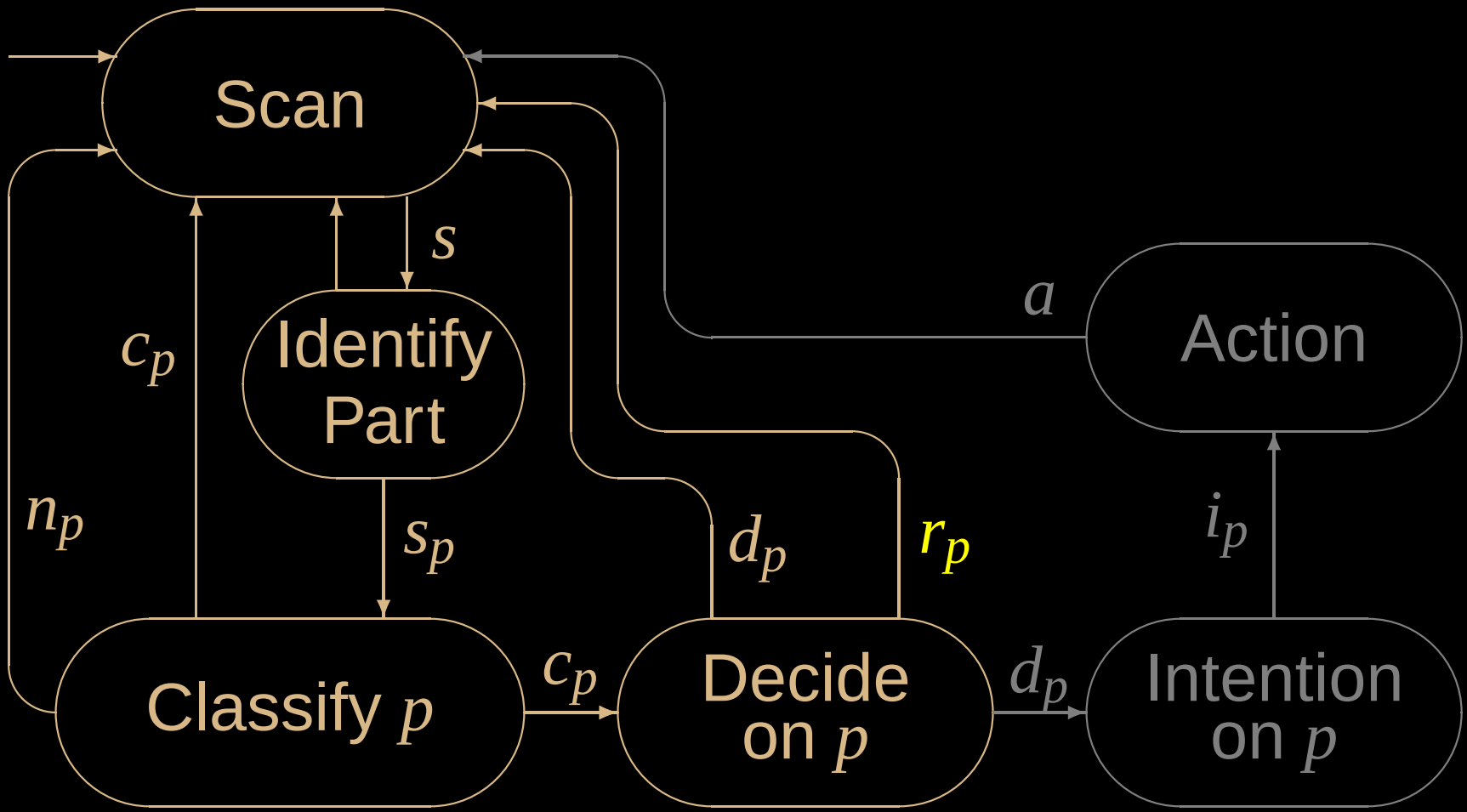
Does the model need to be modified?

- Error Cause: use of the same action name n to denote the results of two cognitive processes
- Change to the model: use action r_p to replace some of the n_p actions.

Solution: New Model



Solution: New Model



Solution: Decomposition?

Does the decomposition need to be modified?

Solution: Decomposition?

Does the decomposition need to be modified?

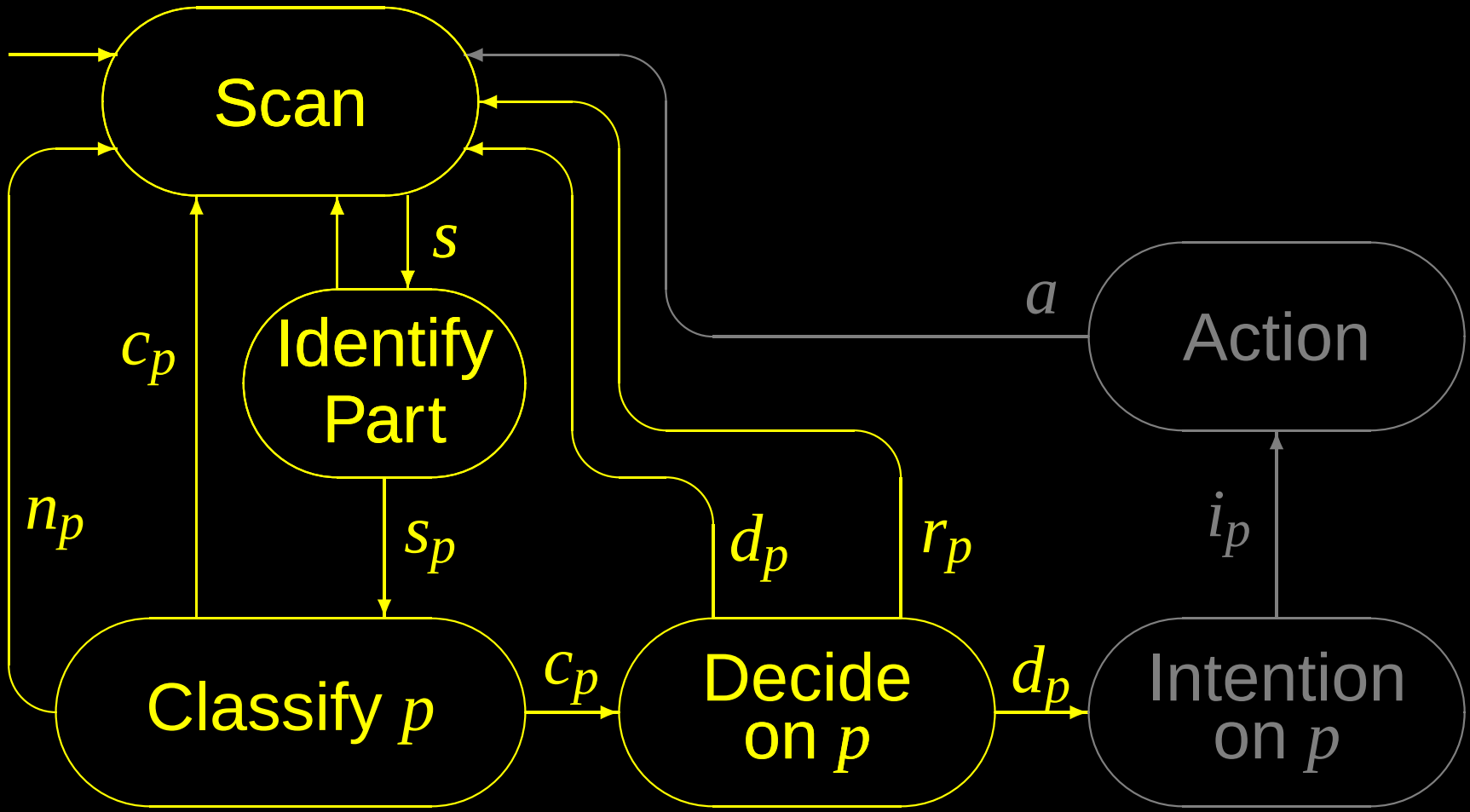
YES!
The decomposition need to cover the counterex-ample

Solution: Completeness

Modify model and/or decomposition to achieve completeness

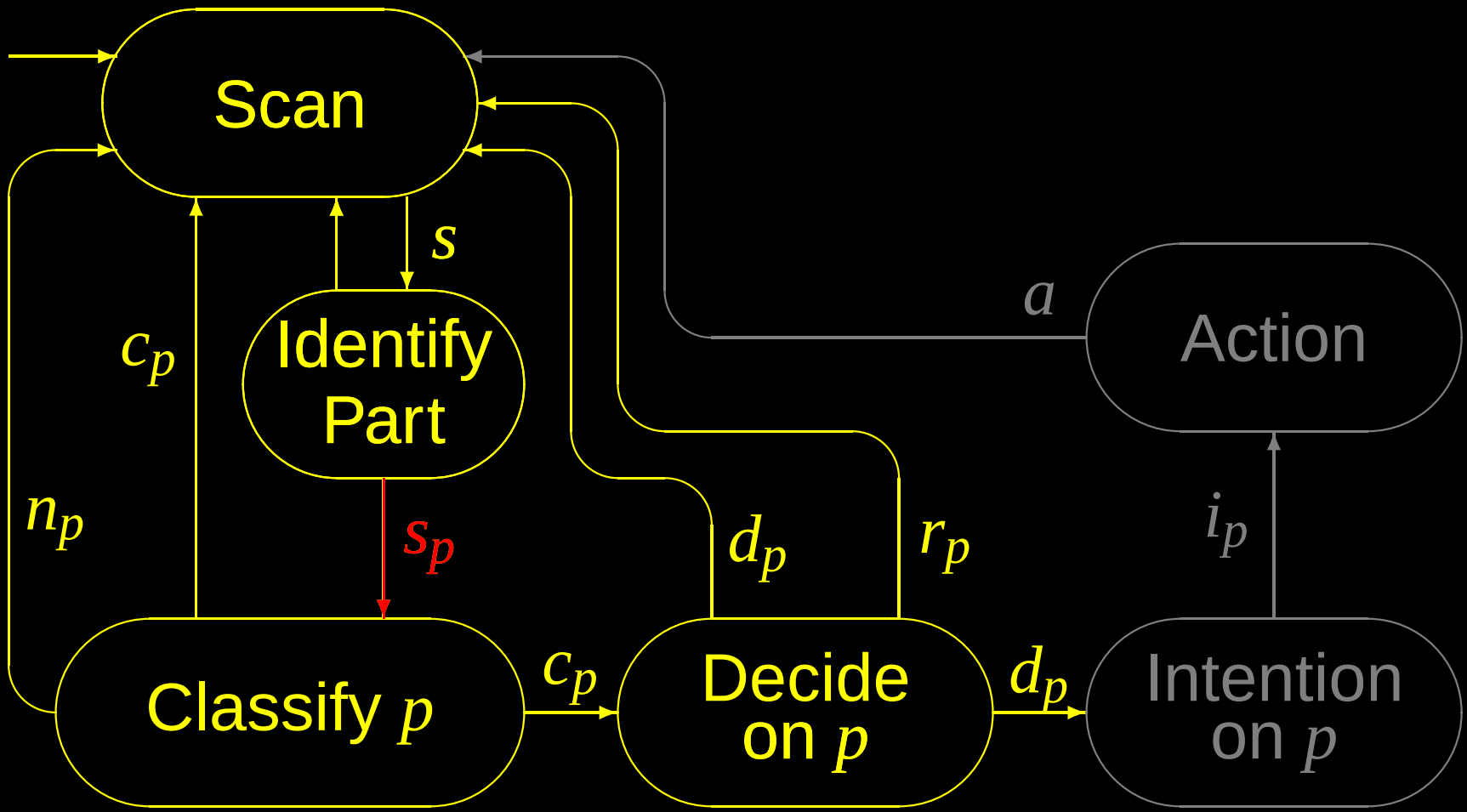
Failure of Scanning

$no\_intended\_response_p$:



Failure of Scanning

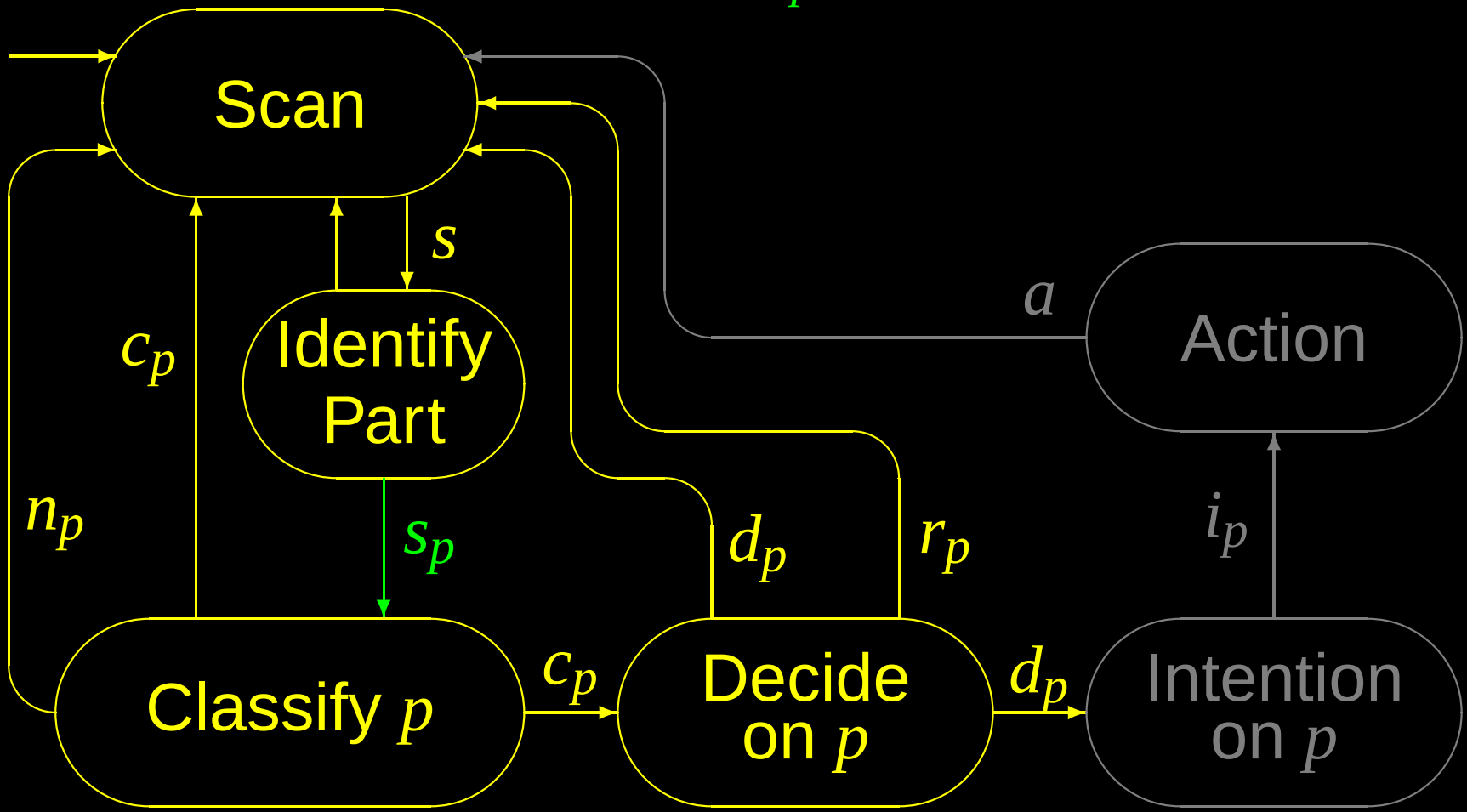
$no\_intended\_response_p$: $\Box \neg s_p$



Failure of Making Decision

$no\_intended\_response_p$: $\Box \neg s_p$

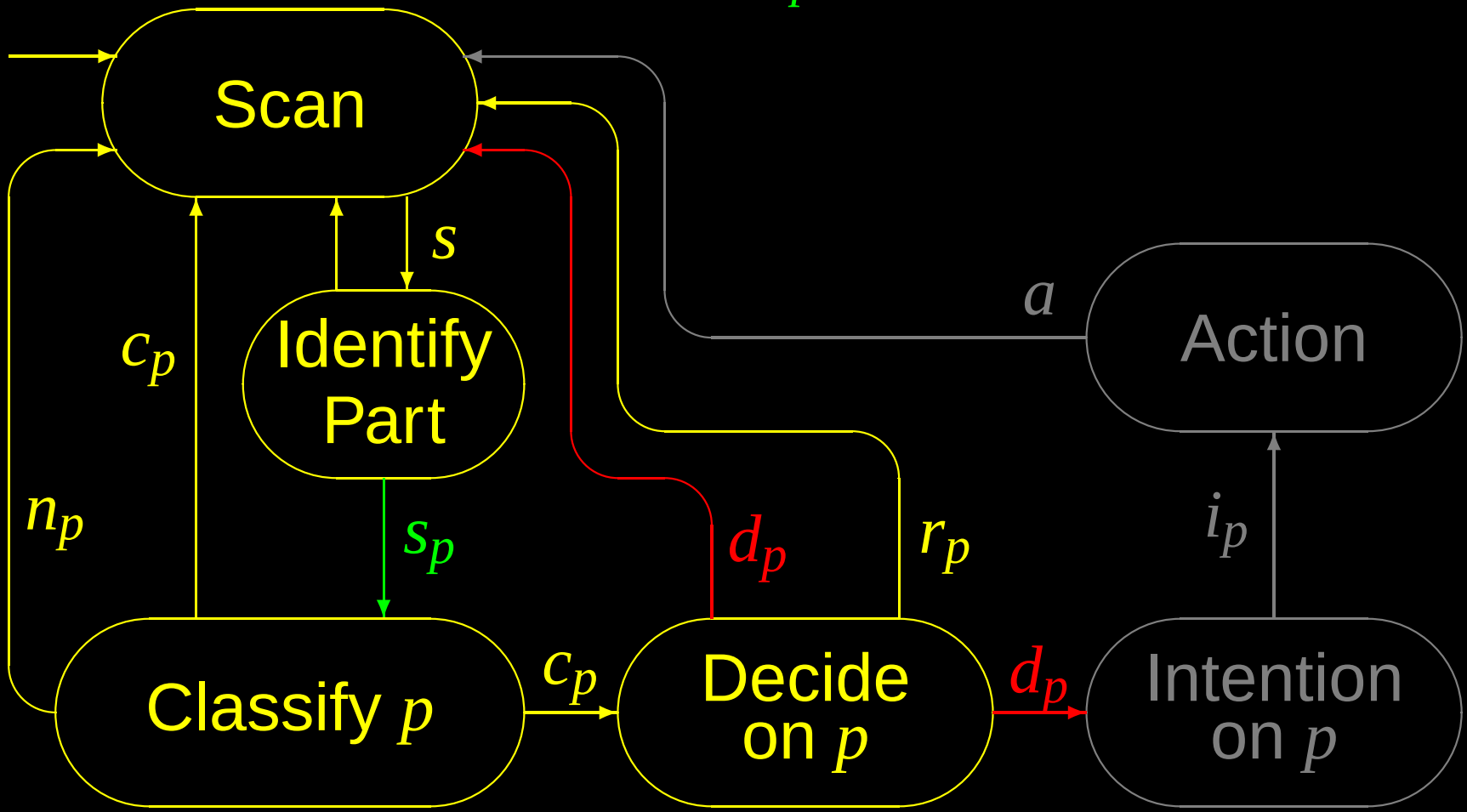
$\Diamond s_p \wedge \ldots$



Failure of Making Decision

$no\_intended\_response_p$: $\Box\neg\, s_p$

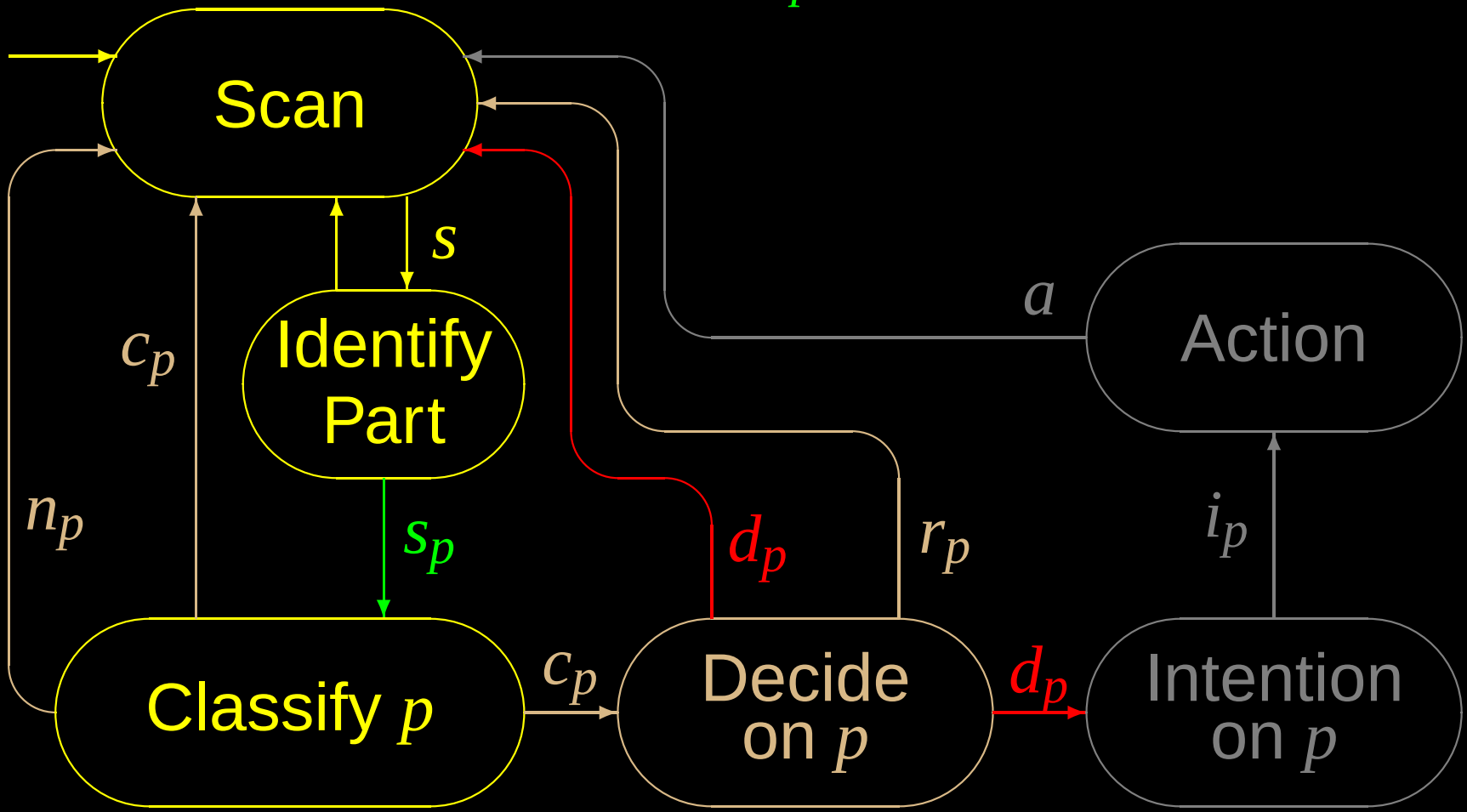
$\Diamond s_p \wedge \ldots$



Persistent Mis-classification

no_intended_response$_p$: $\Box\neg\, s_p$

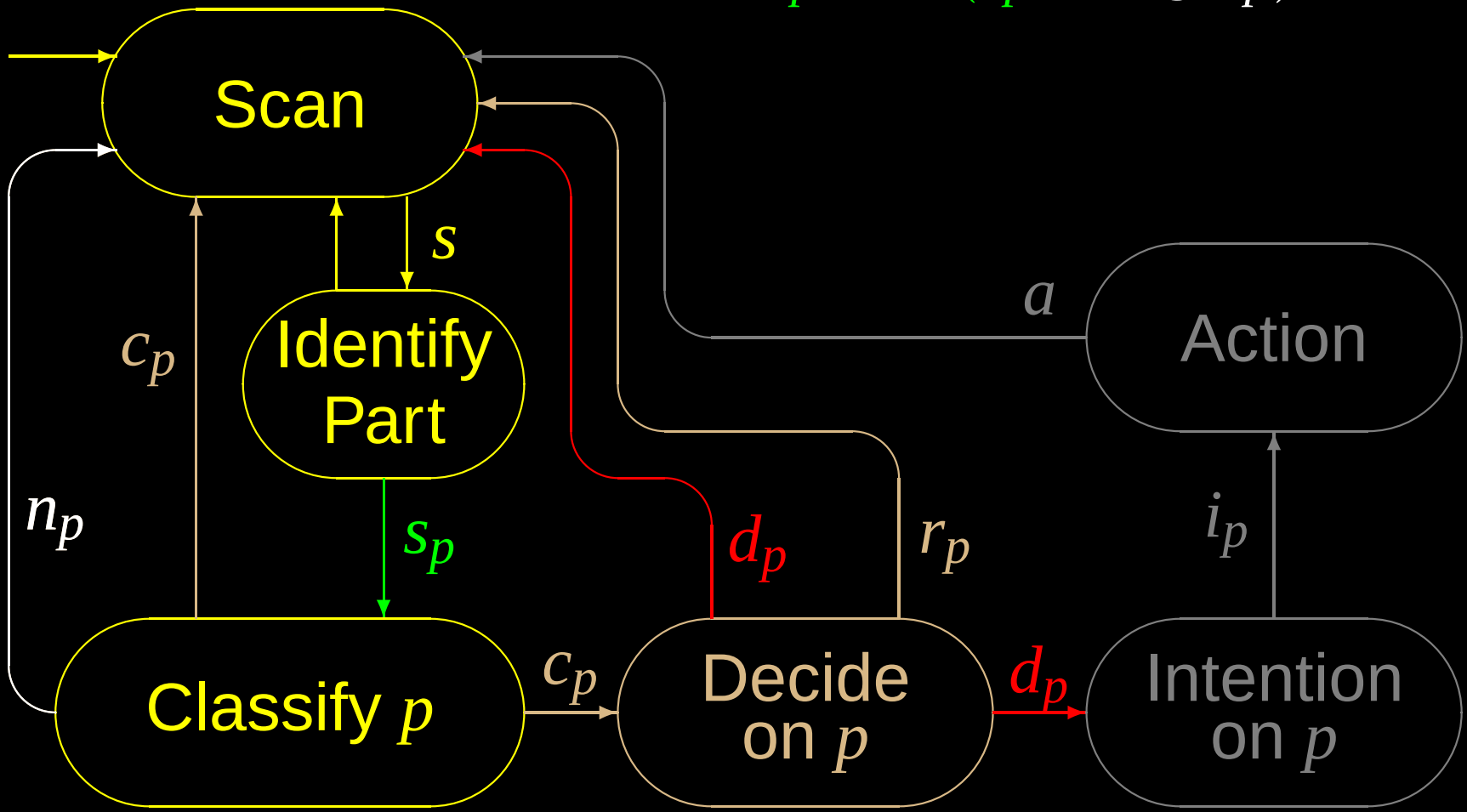
$\Diamond s_p \wedge \ldots$



Persistent Mis-classification

$no\_intended\_response_p$: $\Box\neg\, s_p$

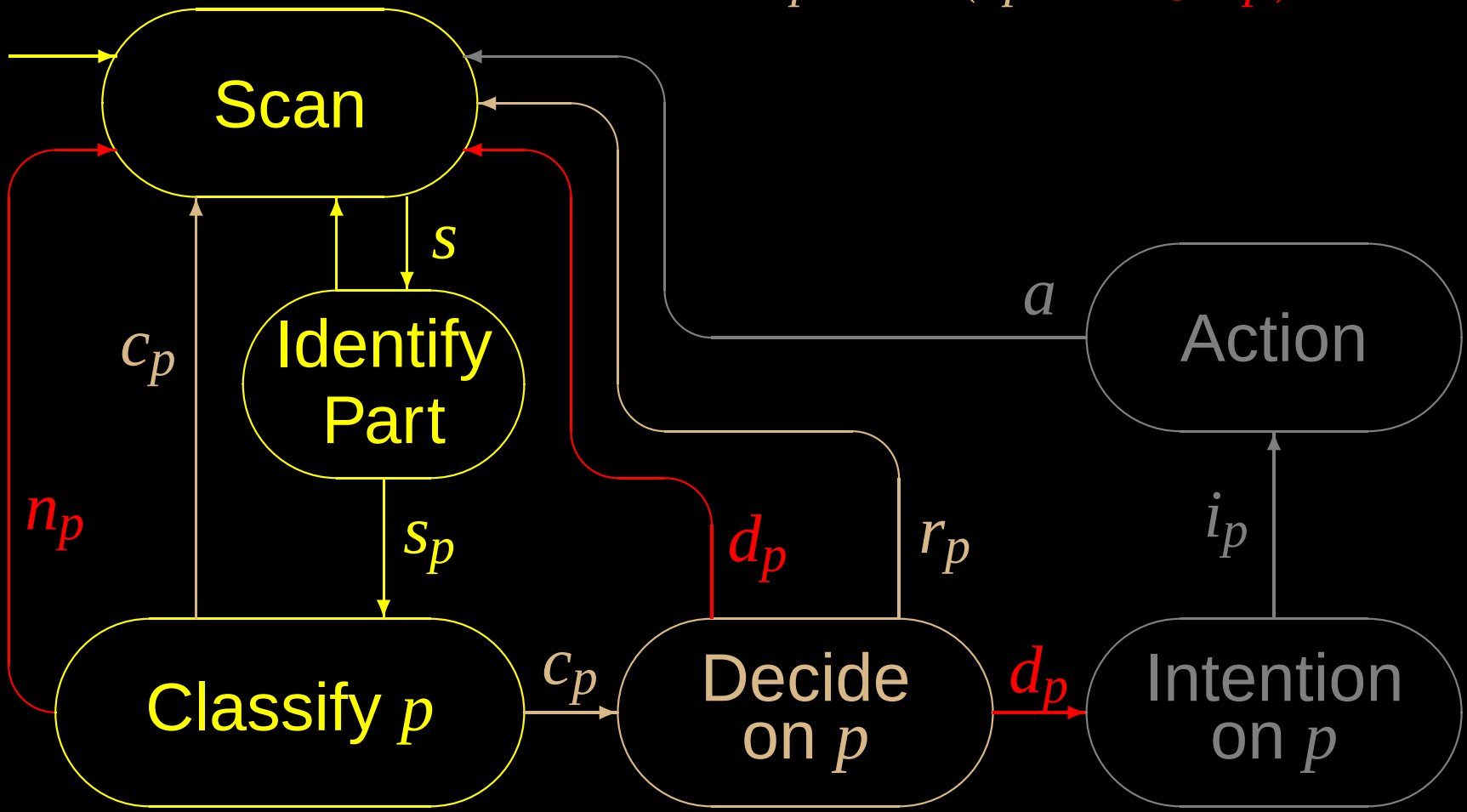
$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$



Persistent Mis-prioritisation

$no\_intended\_response_p$: $\Box\neg\, s_p$

$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$



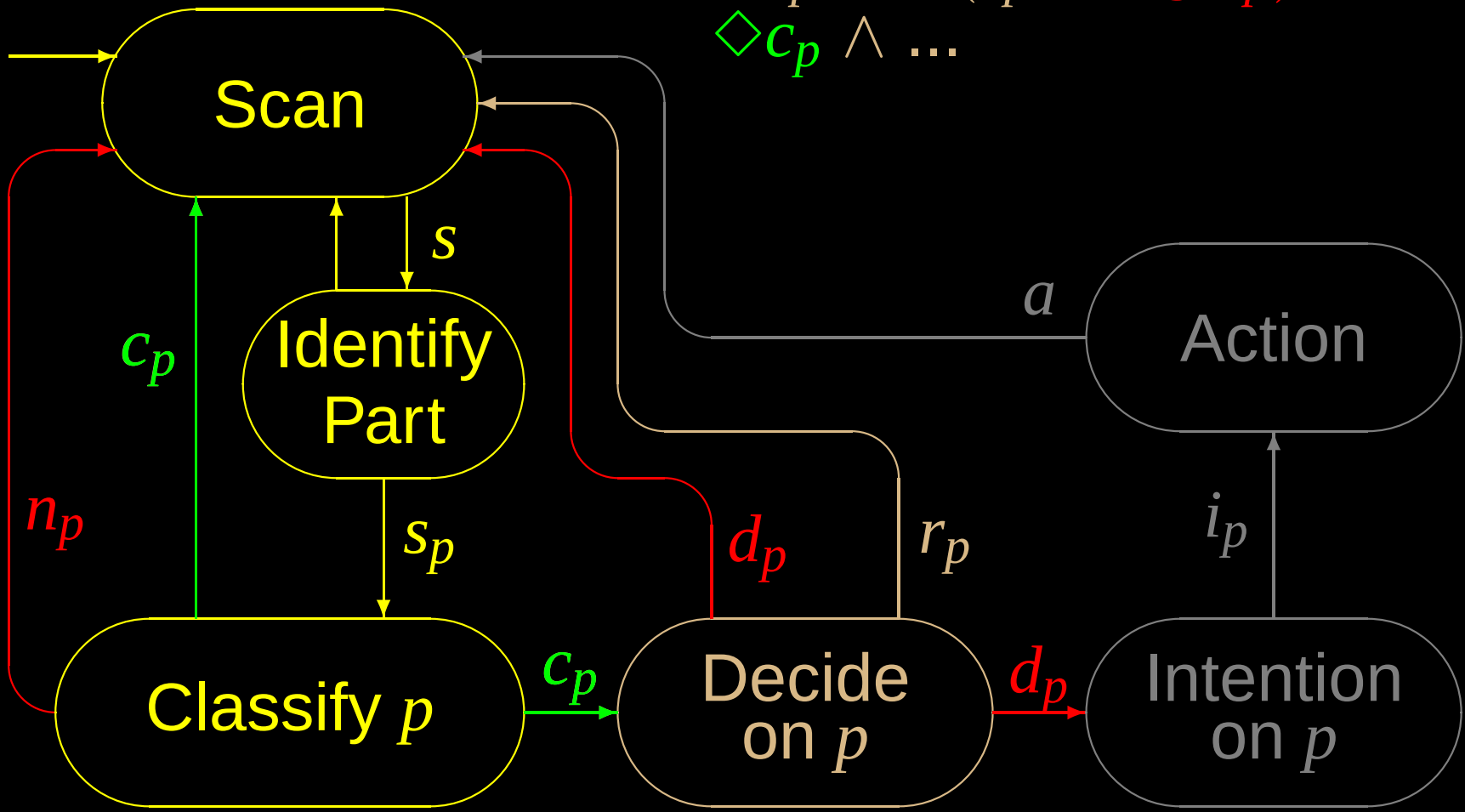
Persistent Mis-prioritisation

$no\_intended\_response_p$:

$\Box\neg\, s_p$

$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$

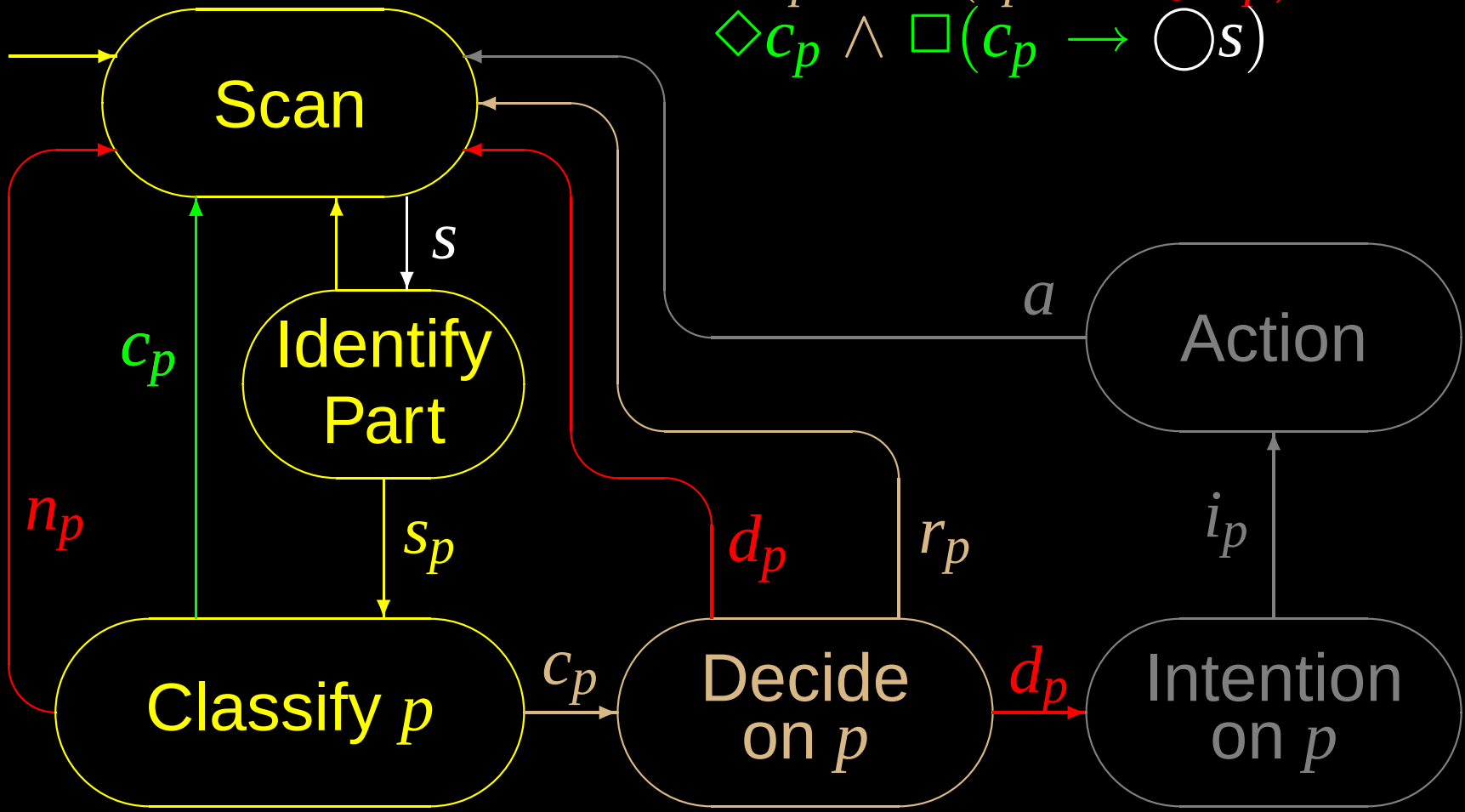
$\Diamond c_p \wedge \ldots$



Persistent Mis-prioritisation

no_intended_response$_p$:

$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$



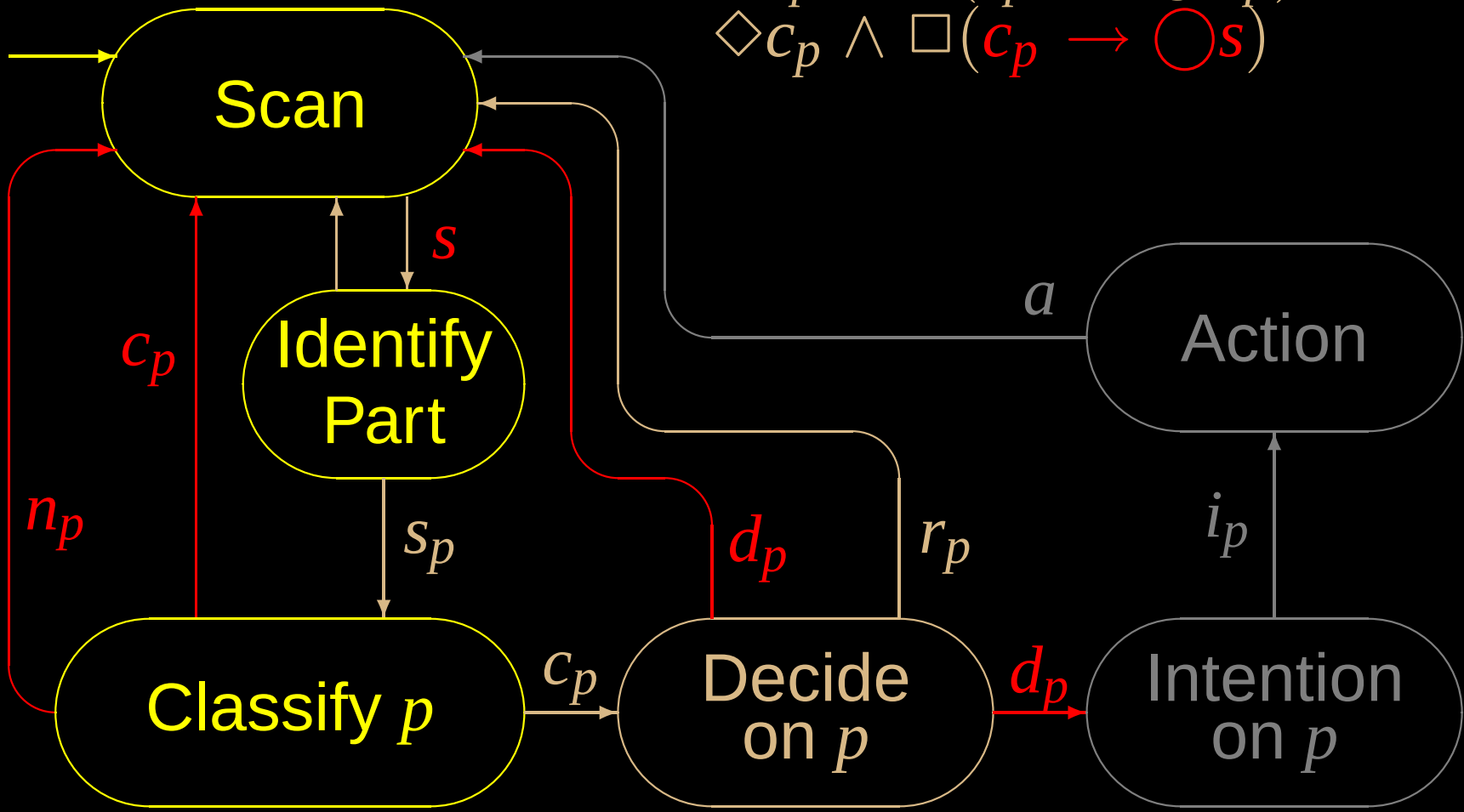
Contrary Decision Process

no_intended_response$_p$:

$\Box\neg\, s_p$

$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$

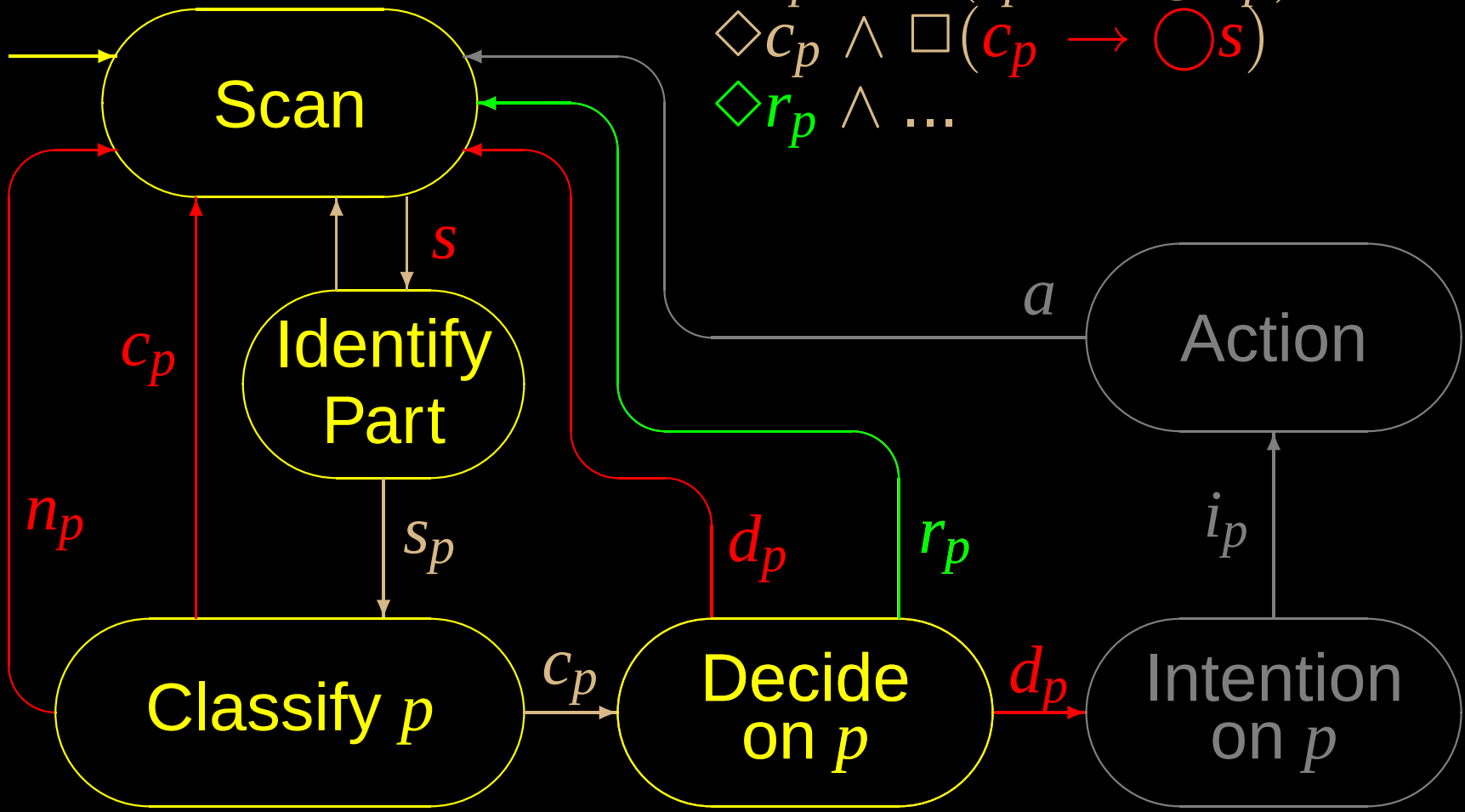
$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$



Contrary Decision Process

$no\_intended\_response_p$:

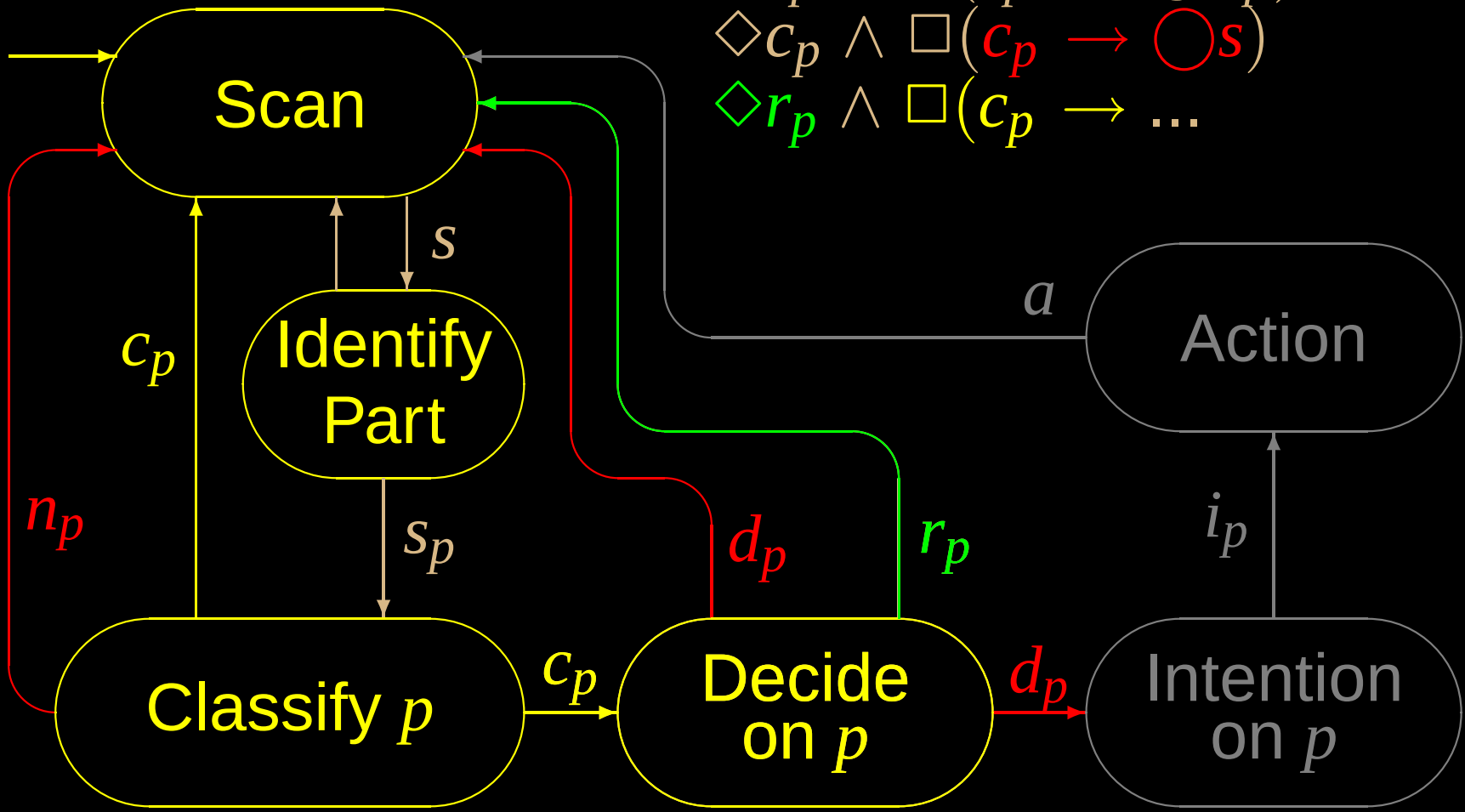
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond r_p \wedge \ldots$$



Contrary Decision Process

$no\_intended\_response_p$:

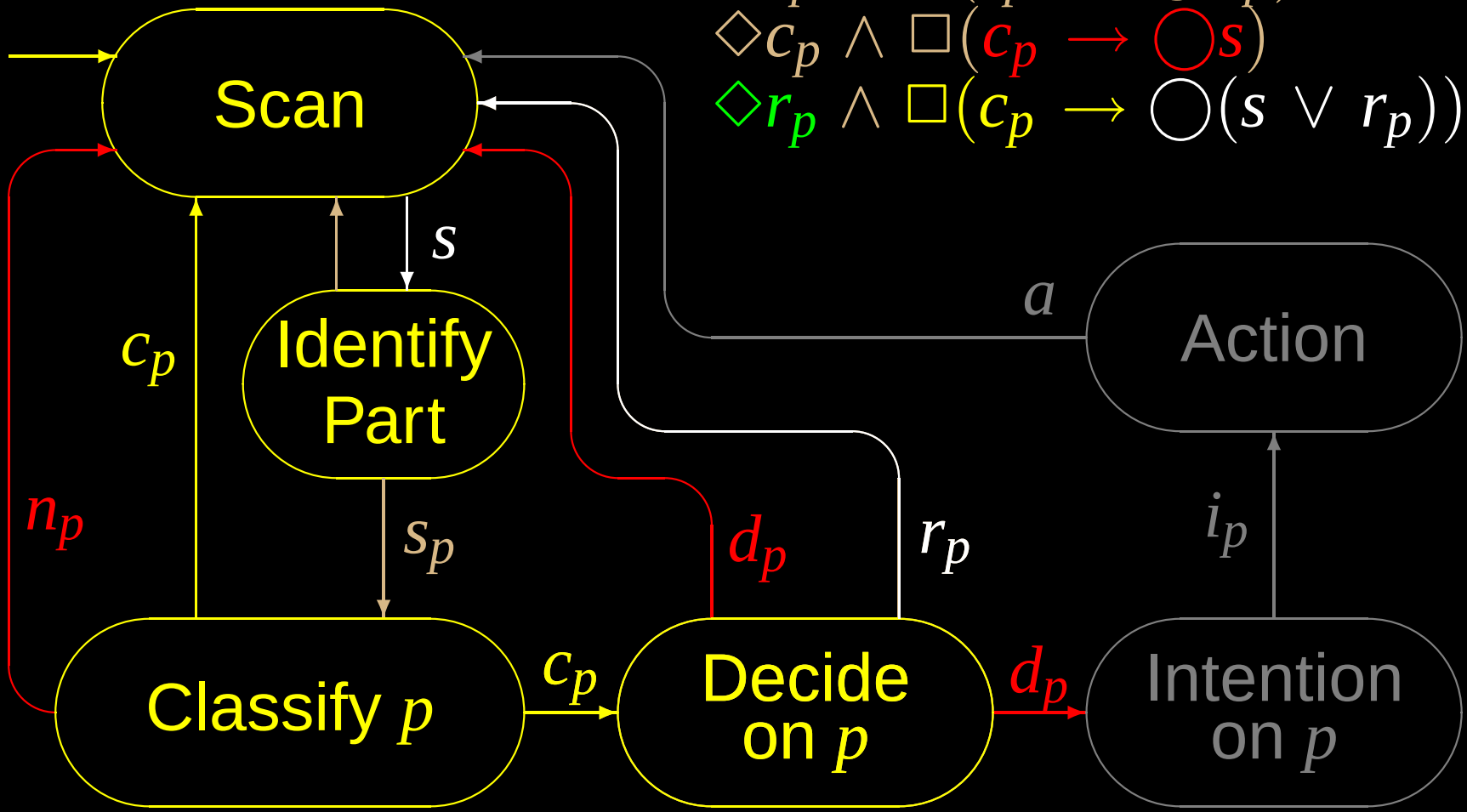
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \ldots$$



Contrary Decision Process

$no\_intended\_response_p$:

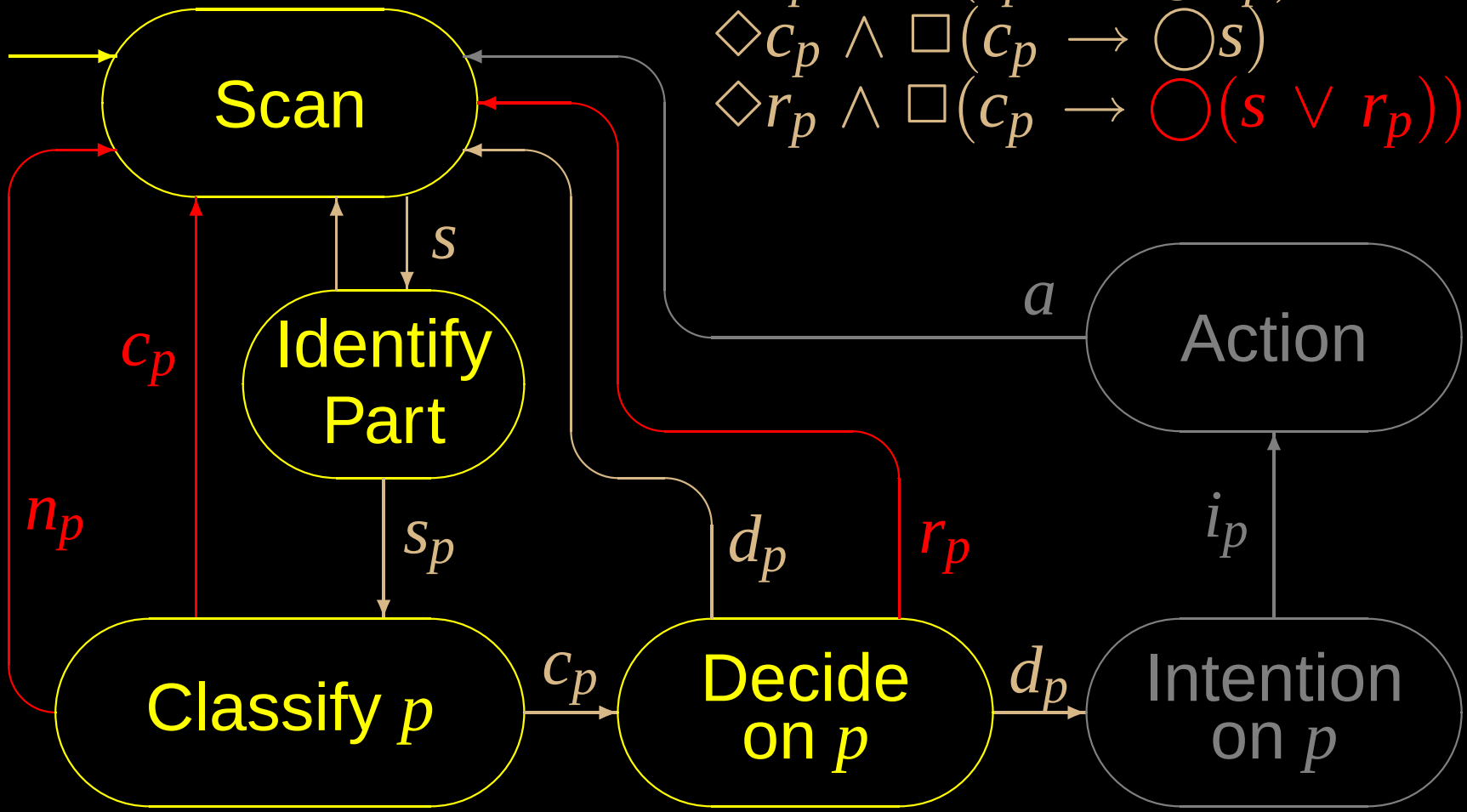
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p))$$



Defer Action for Too Long

no_intended_response$_p$:

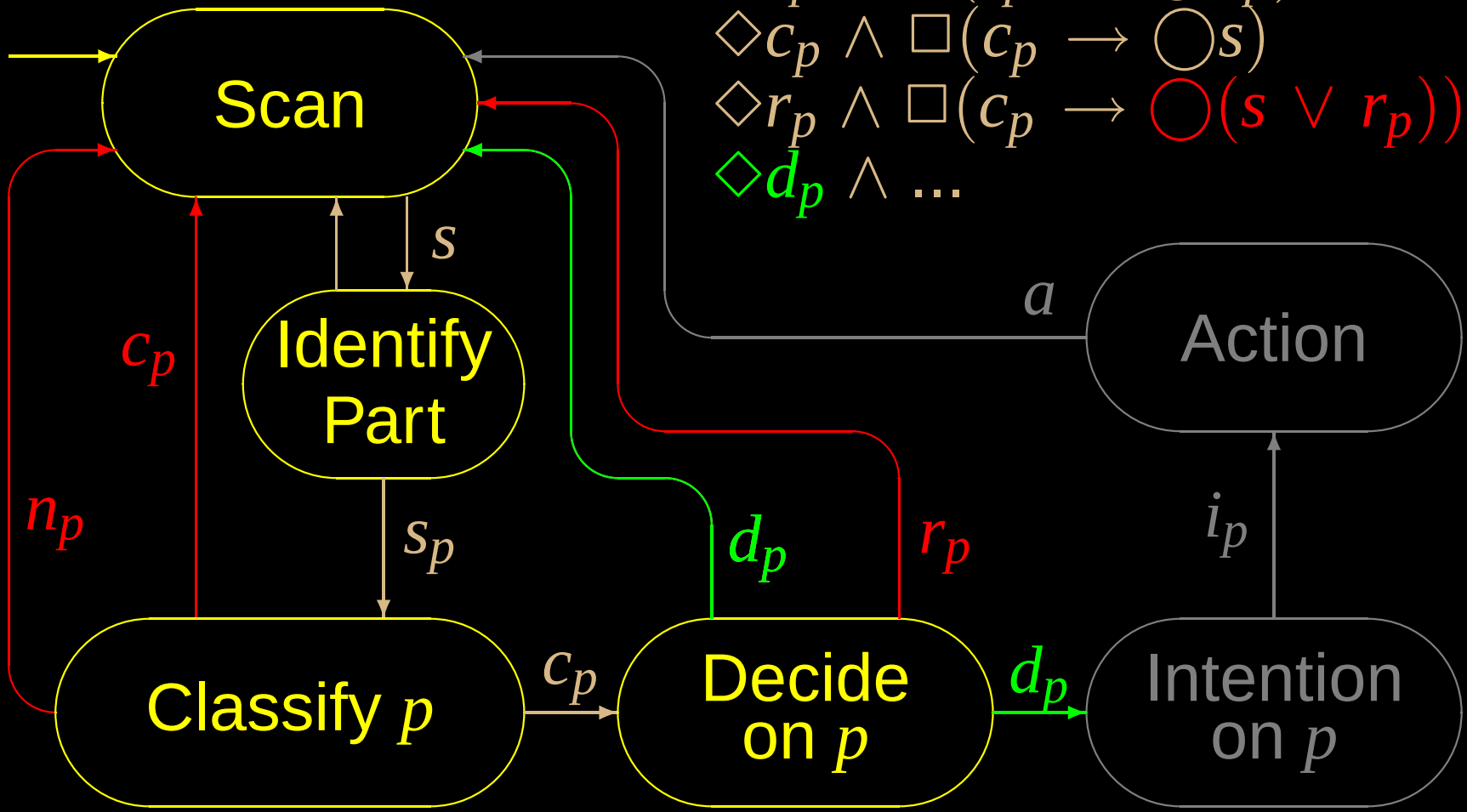
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p))$$



Defer Action for Too Long

$no\_intended\_response_p$:

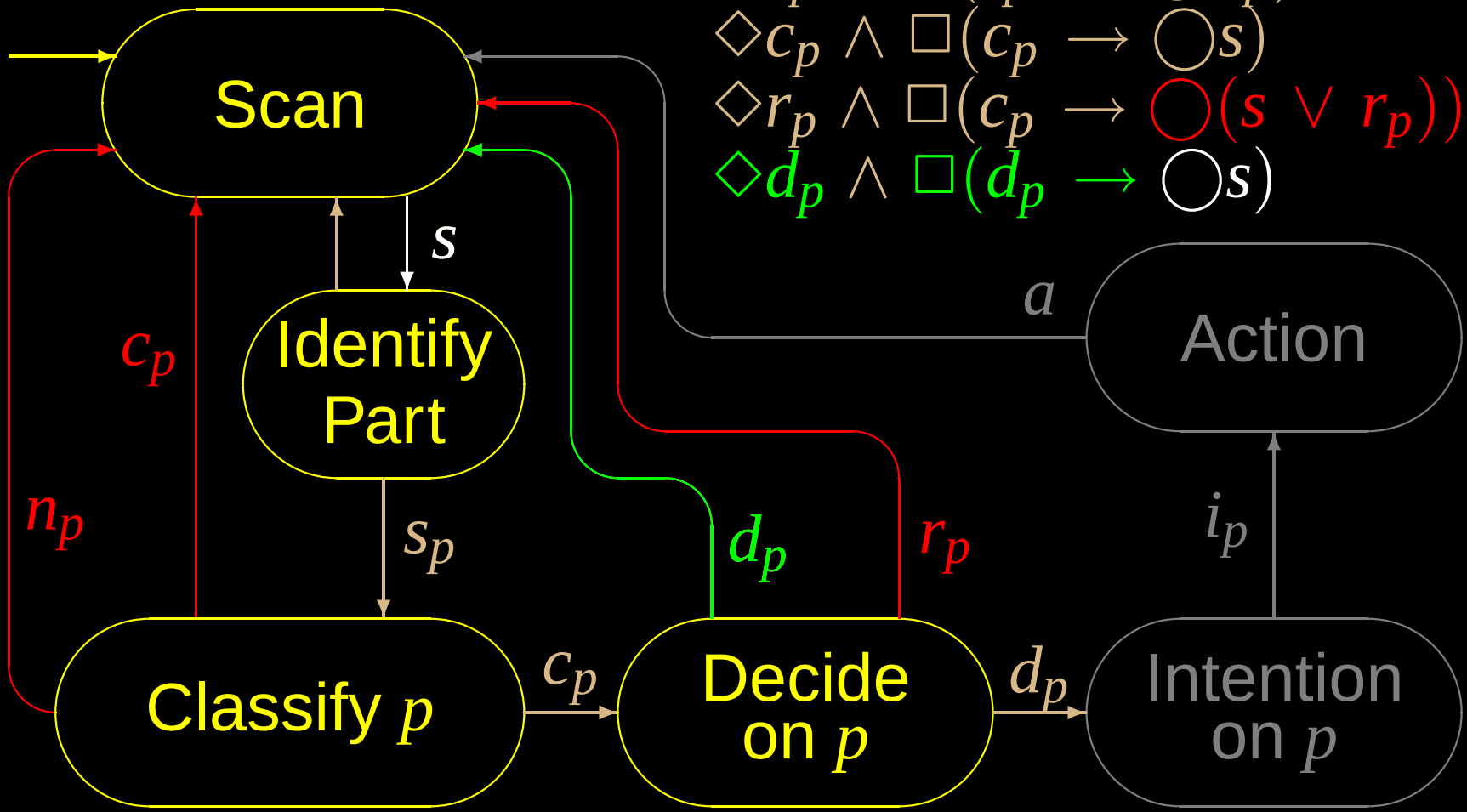
$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p))$$
$$\Diamond d_p \wedge \ldots$$



Defer Action for Too Long

$no\_intended\_response_p$:

$$\Box\neg\, s_p$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p))$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)$$



Final Decomposition

$$\mathcal{D}\ (\mathit{no\_intended\_response}_p) = \{\Box\neg\ s_p\ ,$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)\ ,$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)\ ,$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p))\ ,$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)\ \}$$

Final Decomposition

$$\mathcal{D}\ (\mathit{no\_intended\_response}_p) = \{\Box\neg\ s_p\ ,$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)\ ,$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)\ ,$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p))\ ,$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)\ \}$$

$$\mathcal{D}\ (\mathit{non\_response}_p)$$
$$= \{f \wedge \mathit{non\_resolved}_p \mid f \in \mathcal{D}\ (\mathit{no\_intended\_response}_p)\}$$
$$= \{\Box\neg\ s_p \wedge \mathit{non\_resolved}_p,$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p\ ) \wedge \mathit{non\_resolved}_p,$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s) \wedge \mathit{non\_resolved}_p,$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p)) \wedge \mathit{non\_resolved}_p,$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s) \wedge \mathit{non\_resolved}_p\}$$

Proofs

- Existence of the Task Failures.
- Disjunction of the Task Failures.
- Soundness of the Decomposition.
- Completeness of the Decomposition.

$$OCM \models (\Box \neg\, i_p) \rightarrow \bigvee_{f \in \mathcal{F}} f,$$

where

$$\mathcal{F} = \{fail\_scan_p, pers\_mis\_clas_p, pers\_mis\_prio_p \\ cont\_dec\_proc_p, def\_too\_long_p\}$$

Completeness

$$\Box\neg\, i_p \;\rightarrow\; \bigvee_{f\in\mathcal{F}}\; f$$

where

$$\mathcal{F} \;=\; \mathcal{D}\;(\Box\neg\, i_p) = \mathcal{D}\;(\mathit{no\_intended\_response}_p) =$$
$$\{\; \Box\neg\, s_p\;,$$
$$\Diamond s_p \wedge \Box(s_p \rightarrow \bigcirc n_p)\;,$$
$$\Diamond c_p \wedge \Box(c_p \rightarrow \bigcirc s)\;,$$
$$\Diamond r_p \wedge \Box(c_p \rightarrow \bigcirc(s \vee r_p))\;,$$
$$\Diamond d_p \wedge \Box(d_p \rightarrow \bigcirc s)\;\}$$

Solution: Interpretation

Give a psychological interpretation to the task failure in the correct decomposition

Solution: Interpretation

Give a psychological interpretation to the task failure in the correct decomposition

- Failure of Scanning
- Failure of Making Decision
  - Persistent Mis-classification
  - Persisten Mis-prioritisation
  - Contrary Decision Process
- Defer Action for Too Long

Solution: FS Interpretation

phenotype error: Failure of Scanning

Solution: FS Interpretation

phenotype error: Failure of Scanning

Possible genotype errors are

- tunnel vision: operator looks only at a small portion of the display at a time
- encystment: operator focuses on a single problem and ignores everything else
- vagabonding: operator skipping from problem to problem without spending enough time on each

Solution: FS Interpretation

phenotype error: Failure of Scanning

Possible genotype errors are

- tunnel vision: operator looks only at a small portion of the display at a time
- encystment: operator focuses on a single problem and ignores everything else
- vagabonding: operator skipping from problem to problem without spending enough time on each ($\Longrightarrow$ high workload)

Solution: FS Interpretation

phenotype error: Failure of Scanning

Possible genotype errors are

- tunnel vision: operator looks only at a small portion of the display at a time
- encystment: operator focuses on a single problem and ignores everything else
- vagabonding: operator skipping from problem to problem without spending enough time on each ($\Longrightarrow$ high workload)

Possible design errors:
low resolution or ambiguous display

Solution: PMC Interpretation

- phenotype error: Single Mis-classification

Solution: PMC Interpretation

- phenotype error: Single Mis-classification
  Possible genotype errors
  - failure to project forward correctly
  - mistaken identity
  - belief to have already dealt with the problem

Solution: PMC Interpretation

- phenotype error: Single Mis-classification

  Possible genotype errors

  - failure to project forward correctly
  - mistaken identity
  - belief to have already dealt with the problem

  $\Longrightarrow$ likely recovery

  (project forward eventually wins on memory)

Solution: PMC Interpretation

- phenotype error: Single Mis-classification
  Possible genotype errors
  - failure to project forward correctly
  - mistaken identity
  - belief to have already dealt with the problem

  $\Longrightarrow$ likely recovery
  (project forward eventually wins on memory)
- phenotype error: Persistent Mis-classification
  Possible genotype errors
  - memory may be strengthened $\Longrightarrow$ perception distorted

  due to distraction, similarity with observed non-conflicts, high workload

Solution: PMP Interpretation

- phenotype error: Single Mis-prioritisation

Solution: PMP Interpretation

- phenotype error: Single Mis-prioritisation
  Possible genotype errors are
  - mis-calculation
  - mis-storage
  - mis-retrival

  of the time planned for corrective actions

Solution: PMP Interpretation

- phenotype error: Single Mis-prioritisation
  Possible genotype errors are
  - mis-calculation
  - mis-storage
  - mis-retrival

  of the time planned for corrective actions $\Longrightarrow$
  possible recovery
  (through new calculation at a next scan)

Solution: PMP Interpretation

- phenotype error: Single Mis-prioritisation
  Possible genotype errors are
  - mis-calculation
  - mis-storage
  - mis-retrival

  of the time planned for corrective actions $\Longrightarrow$
  possible recovery
  (through new calculation at a next scan)
- phenotype error: Persistent Mis-prioritisation
  Possible genotype errors
  - memory of result of previous mis-calculation keeps emerging

Solution: CDP Interpretation

- phenotype error: Single Mis-reclassification

Solution: CDP Interpretation

- phenotype error: Single Mis-reclassification

  Possible genotype errors are

  - mis-calculation
  - mis-storage
  - mis-retrival

  during the decision process

Solution: CDP Interpretation

- phenotype error: Single Mis-reclassification
  Possible genotype errors are
  - mis-calculation
  - mis-storage
  - mis-retrival

  during the decision process $\Longrightarrow$ possible recovery
  (through new calculation at a next scan)

Solution: CDP Interpretation

- phenotype error: Single Mis-reclassification
  Possible genotype errors are
  - mis-calculation
  - mis-storage
  - mis-retrival

  during the decision process $\Longrightarrow$ possible recovery
  (through new calculation at a next scan)
- phenotype error: Contrary Decision Process
  Possible genotype errors
  - memory of previous decisions on similar pairs resulting in unnecessary actions

  due to fear, high workload

Solution: DATL Interpretation

- phenotype error: Single Mis-deferring Action

Solution: DATL Interpretation

- phenotype error: Single Mis-deferring Action
  Possible genotype errors are
  - mis-calculation of time
  - mis-retrival of intention
  - slip

Solution: DATL Interpretation

- phenotype error: Single Mis-deferring Action
  Possible genotype errors are
  - mis-calculation of time
  - mis-retrival of intention
  - slip

  $\Longrightarrow$ possible recovery
  (through new decision process at a next scan)

Solution: DATL Interpretation

- phenotype error: Single Mis-deferring Action
  Possible genotype errors are
  - mis-calculation of time
  - mis-retrival of intention
  - slip

  $\Longrightarrow$ possible recovery
  (through new decision process at a next scan)
- phenotype error: Defer Action for Too Long
  Possible genotype errors
  - persistent mis-retrival of intention and closure of the decision process

  due to very high workload

Model-checking Results

- Negative result of the validity checking on the completeness of an initially attempted decomposition.

Model-checking Results

- Negative result of the validity checking on the completeness of an initially attempted decomposition.
- Changes to the Model: in particular, it has been enriched with r_p.

Model-checking Results

- Negative result of the validity checking on the completeness of an initially attempted decomposition.
- Changes to the Model: in particular, it has been enriched with r_p.
- Changes to the Specification: in particular, the the newly defined *contrary decision process* task failure has been added to the decomposition.

Model-checking Results

- Negative result of the validity checking on the completeness of an initially attempted decomposition.
- Changes to the Model: in particular, it has been enriched with r_p.
- Changes to the Specification: in particular, the the newly defined *contrary decision process* task failure has been added to the decomposition.
- Psychological interpretation of the new task failure.

Examination — ATC

Operator Choice Model and Mode Confusion

- Seminars
  - Full OCM model for the ATC
  - Formal analysis of mode confusion
- Reports
  - Formal model of the full OCM for ATC
  - Formal analysis of Cooperative Task Models

Examinations

Seminar 1 — Full OCM for ATC

Topic: Operator Choice Model for ATC

Full OCM model for the ATC

- D. Leadbetter, P. Lindsay, A. Hussey, A. Neal and M. Humphreys Towards Towards Model Based Prediction of Human Error Rates in Interactive Systems, 2000
- A. Hussey, D. Leadbetter, P. Lindsay, A. Neal and M. Humphreys Modelling and Hazard Identification in an Air-Traffic Control User-Interface, 2000
- S. Connelly, P. Lindsay, A. Neal and M. Humphreys A formal model of cognitive processes for an Air Traffic Control Task, 2001

Seminar 2 — Mode Confusion

Topic: Mode Confusion

Formal analysis of mode confusion

- S. P. Miller and J. N. Potts
  Detecting Mode confusion Through formal Modelling and Analysis, 1999
- N. Leveson, L. D. Pinnel, S. D. Sandys, S. Koga and J. D. Reese
  Analysing Software Specification for Mode Confusion Potential, 1998
- R. W. Butler, S. P. Miller, J. N. Potts and V. A. Carreno
  A Formal Methods Approach to the Analysis of Mode Confusion, 1998

Report 1 — FM of Full ATC

Topic: Operator Choice Model

Formal model of the full OCM for ATC

using CSP or other formalism, possibly running simulation using a tool

- D. Leadbetter, P. Lindsay, A. Hussey, A. Neal and M. Humphreys
  Towards Model Based Prediction of Human Error Rates in Interactive Systems, 2000
- S. Connelly, P. Lindsay, A. Neal and M. Humphreys
  A formal model of cognitive processes for an Air Traffic Control Task, 2001
- Antonio Cerone, Simon Connelly and Peter Lindsay.
  Formal Analysis of Operator Behavioural Patterns in Interactive Systems, submitted

Report 2 — Cooperative TM

Topic: Task Models

Formal Analysis of Cooperative Task Models

Discussion of the papers' differences and limitations and propose possible extensions

- F. Paternò, C. Santoro and S. Thamassebi
  Formal models for Cooperative Tasks: Concepts and an Application for En-route Air Traffic Control
- V. M. R. Penichlet, F. Paternò, J. A. Gallud and M. D. Lozano
  Collaborative Social Structures and Task Modelling Integration
- D. Pinelle and C. Gutwin
  Task Analysis for Groupware Usability Evaluation: Modeling Shared Workplace Tasks with Mechanics of cCllaboration

Demo

References