DUTCH
SAFETY BOARD

Using STAMP to investigate decision-making

a DSB ~~Case Study~~ Proposal

Introducing the Dutch Safety Board

- Investigation of (near-) incidents
- Blame-free, focus on learning
- Government-funded, independent
- All industries, various types of safety
- 3 board members
- ~40 investigators
- ~12 full-scale investigations per year

www.safetyboard.nl

(many reports also available in English)

A typical DSB investigation

- Accident
- Findings
  - No or minor performance problems at the operational level; machines and humans (try to) do a good job *within the environment provided to them*
  - Unsafety arises from (in)action at managerial / governance / oversight level, resulting in conflicting set points, inadequate allocation of resources, absence of effective feedback mechanisms etc.
- Conclusion
  - Safety should figure more prominently in managerial action / corporate governance / public oversight

The issue

- Isn’t this a lot like saying “pilot error”, only at the managerial / oversight level?
- Shouldn’t we try to explain high-level control failure instead, so control can be improved?
- Can STAMP/STPA be of use?
- (yes, yes and yes)

Aim

- Concentrating on decision-making,
- Show how STAMP/STPA facilitates a systematic investigation into control failure
- Propose a generic model for doing his (D-STPA)
- ~~Show how well this works~~

Decision-making

- Generic, high-level means of control
- Typically concerning strategic goals (set points)
- Typically a precondition for deployment of other managerial controls (budget allocation etc)
- Recognizable process, formalized to some extent
- Involving conscious deliberation to some extent
- Not to be equated with *deciding* (cognitive operation)

- A better, more concise definition is still needed

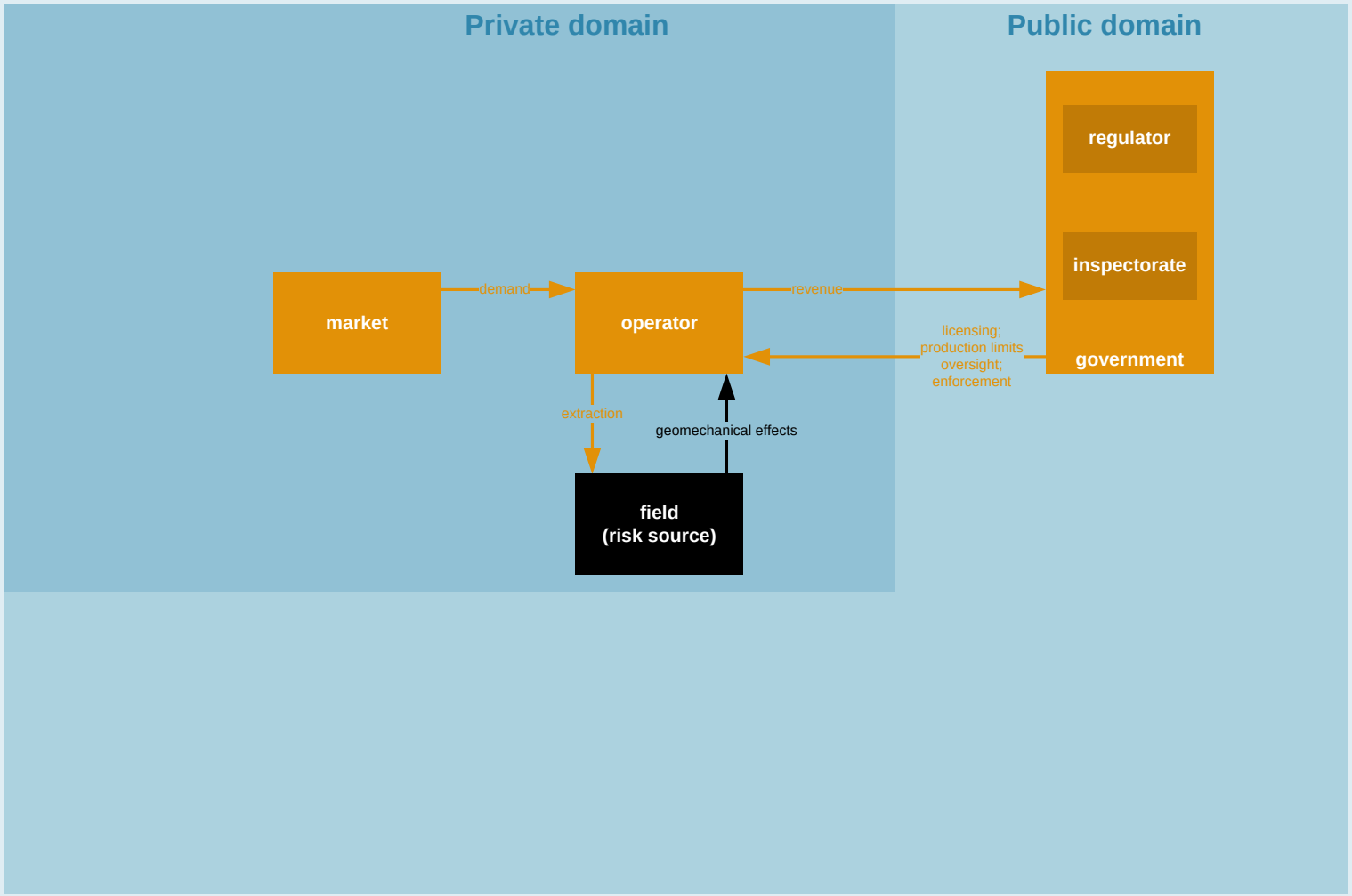
Case description

- Increase of seismic events of increasing severity
- Related to extraction of natural gas from Groningen field (onshore)
- Safety of inhabitants may be at risk (disputed)
- Safety concerns among inhabitants

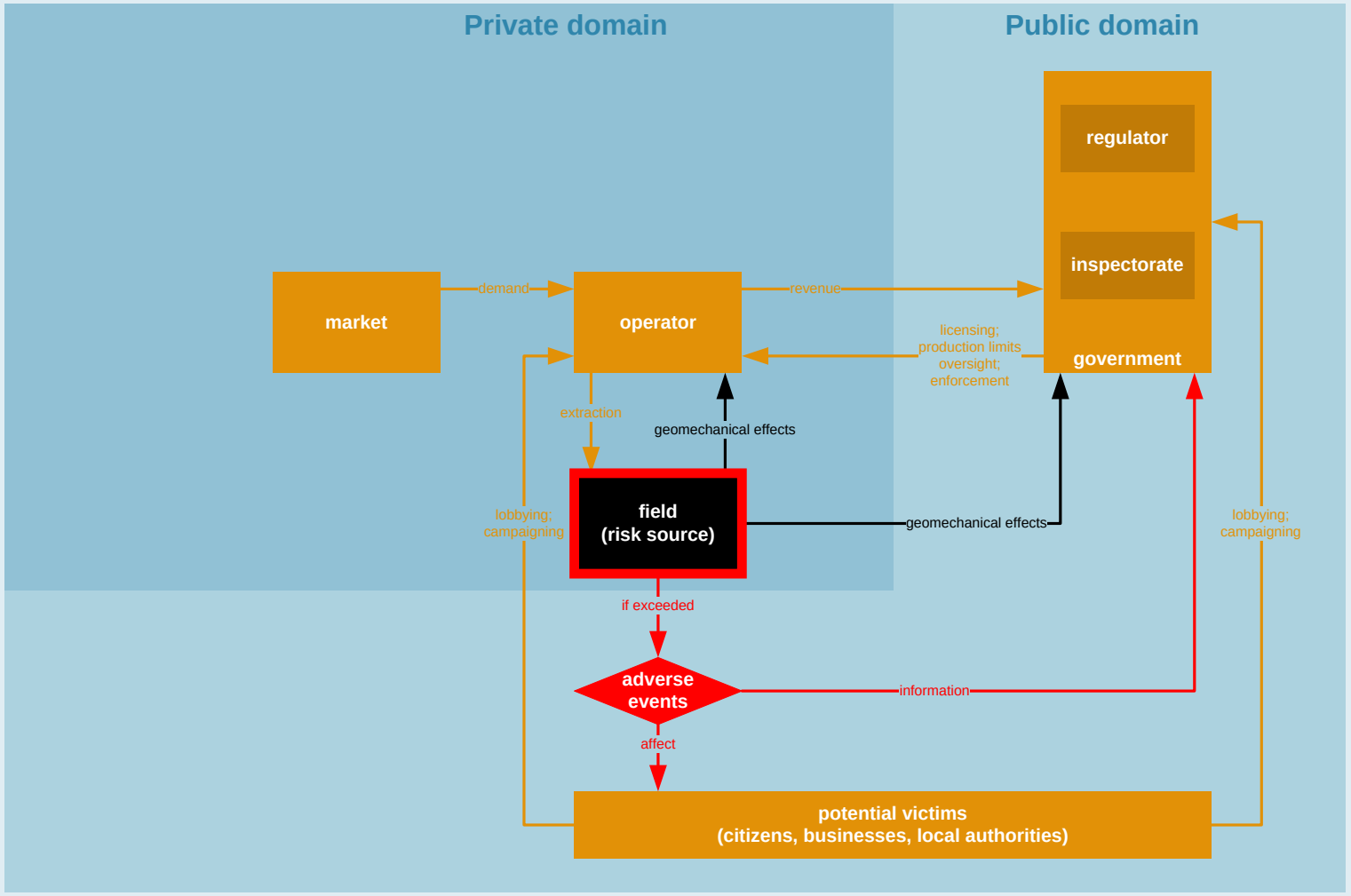
What role has safety played in the exploitation of the Groningen field?

Focus on ~~operational~~ strategic aspects

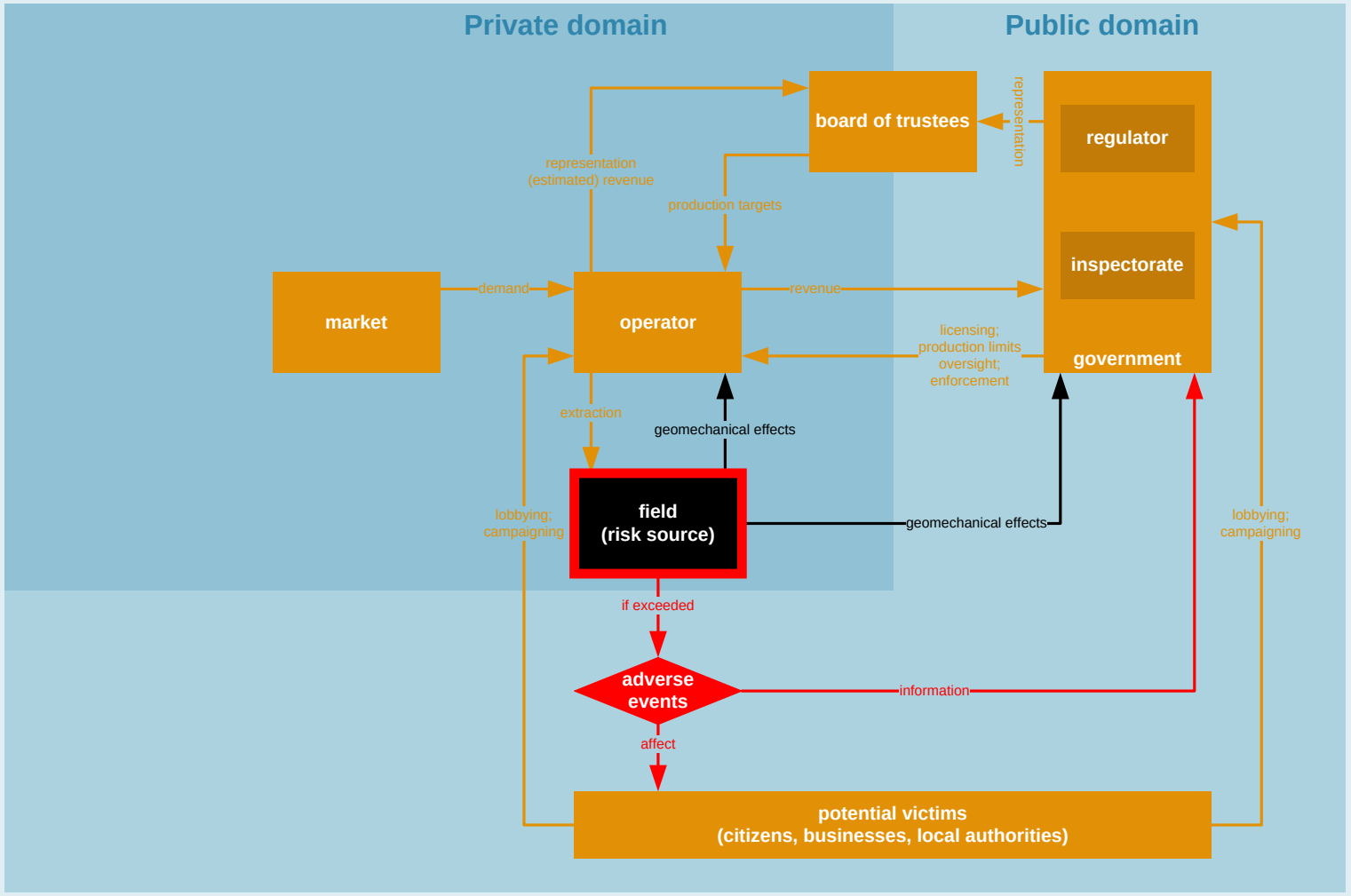
Gas extraction – control structure



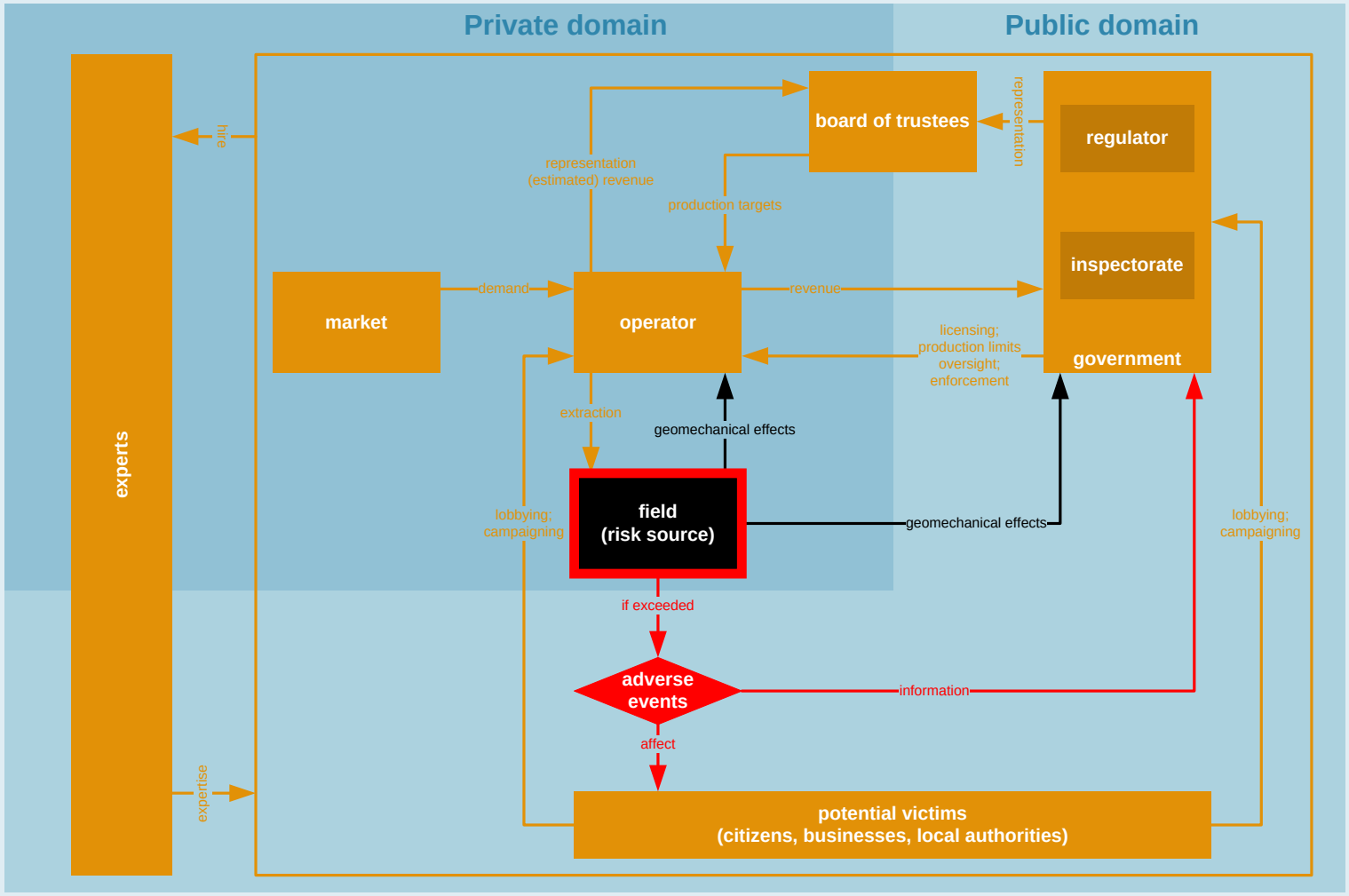
Gas extraction – control structure



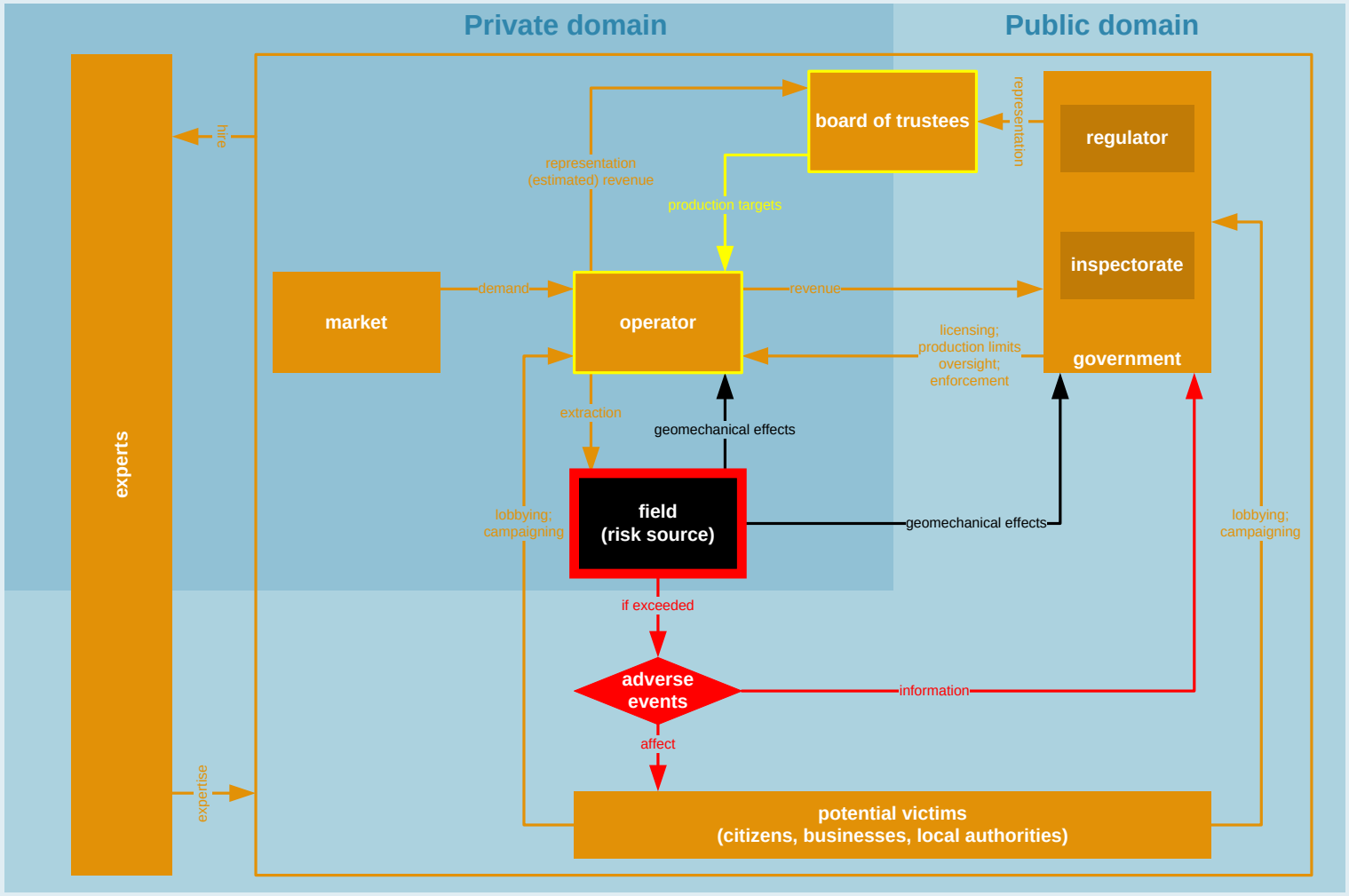
Gas extraction – control structure



Gas extraction – control structure



Gas extraction – control structure



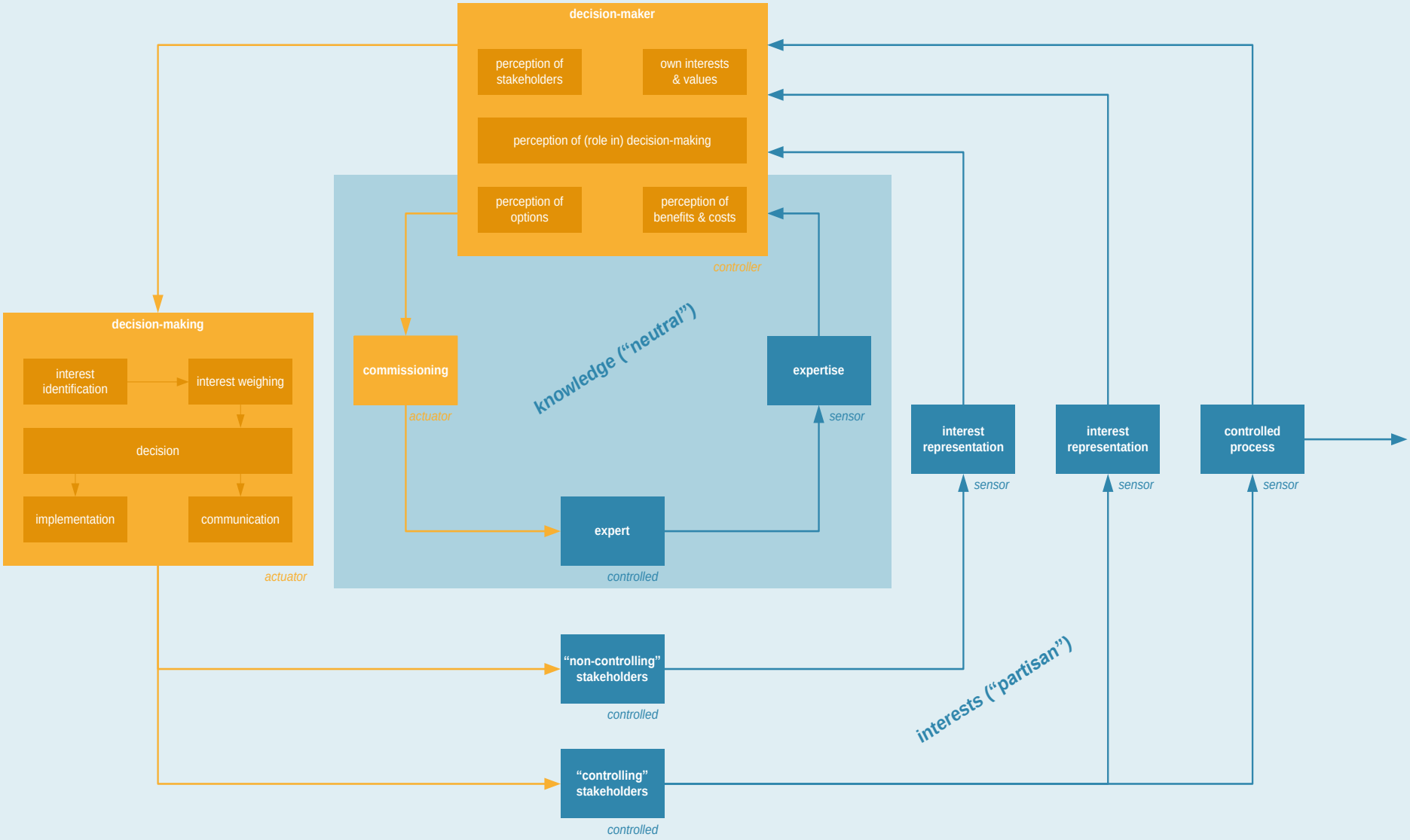
Control Characteristics

- Controller is only in charge of choosing set point, not other typical management controls
- Controller is not a single person
- Controller is positioned outside organisation controlling the hazardous process
- Controller has to consider conflicting interests

Introducing D-STPA

- “Standard” STPA thinking, applied to decision-making
- Informed by management/governance lit
- Generic; applicable to many decision-making processes
- Key features
  - Decision-making = actuator, operated by decision-maker (=controller) to control stakeholders
  - Stakeholders attempt to control DM by means of interest representation (modelled as a sensor)
  - Interest representation is inherently partisan → DM will typically also seek ‘objective’ third-party expertise

Introducing D-STPA

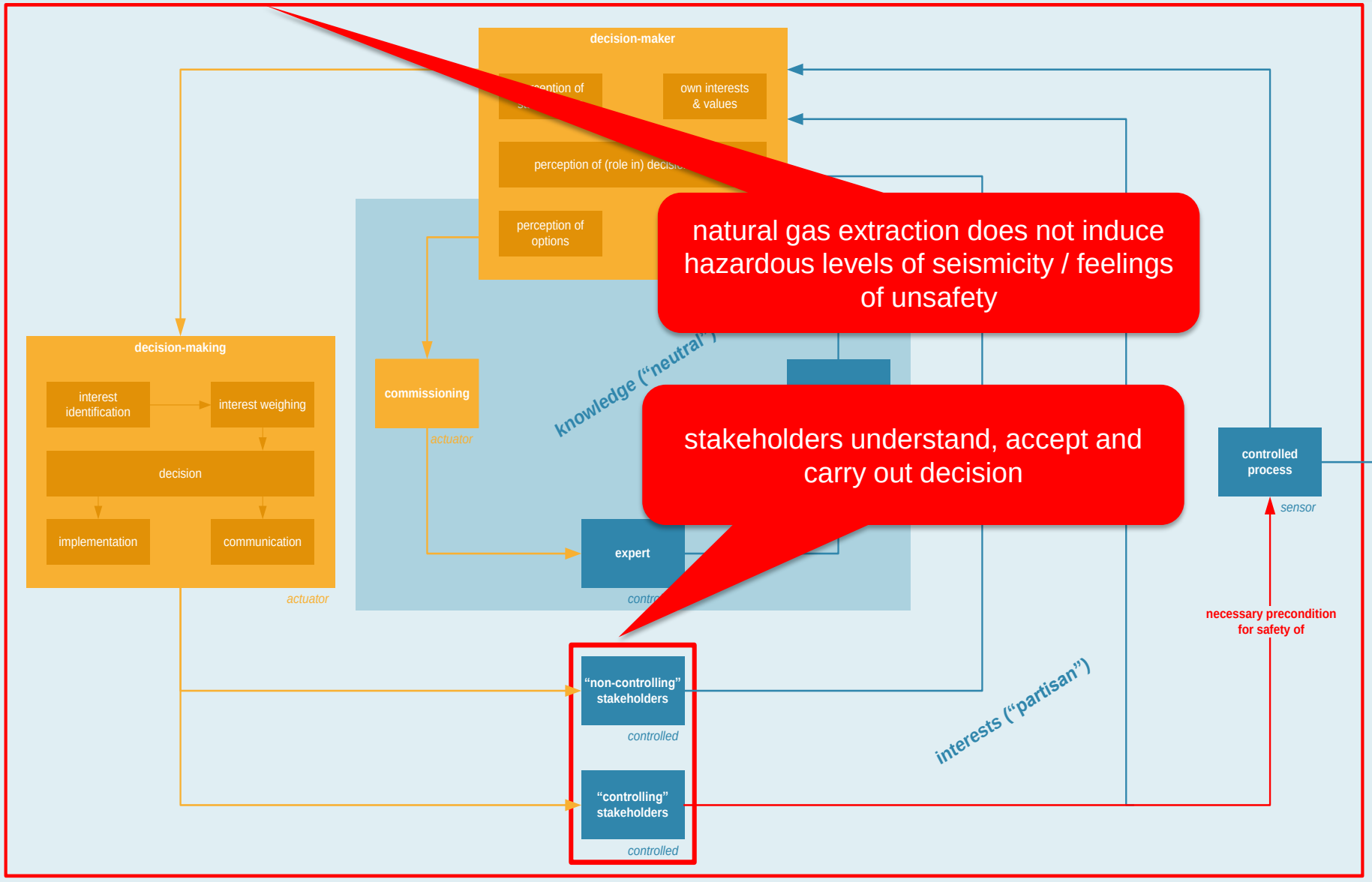


Rational safety vs perceived safety

- DM controls two kinds of stakeholders
  - Controlling stakeholders, who control potentially hazardous processes
  - Non-controlling stakeholders, including potential victims of these processes

- Successful control by DM results in
  - Controlling stakeholders understanding and executing DM's decision, which is a precondition for safety in the underlying process (rational safety)
  - Non-controlling stakeholders understanding and accepting DM's decision, which is a precondition for their feeling safe (perceived safety)

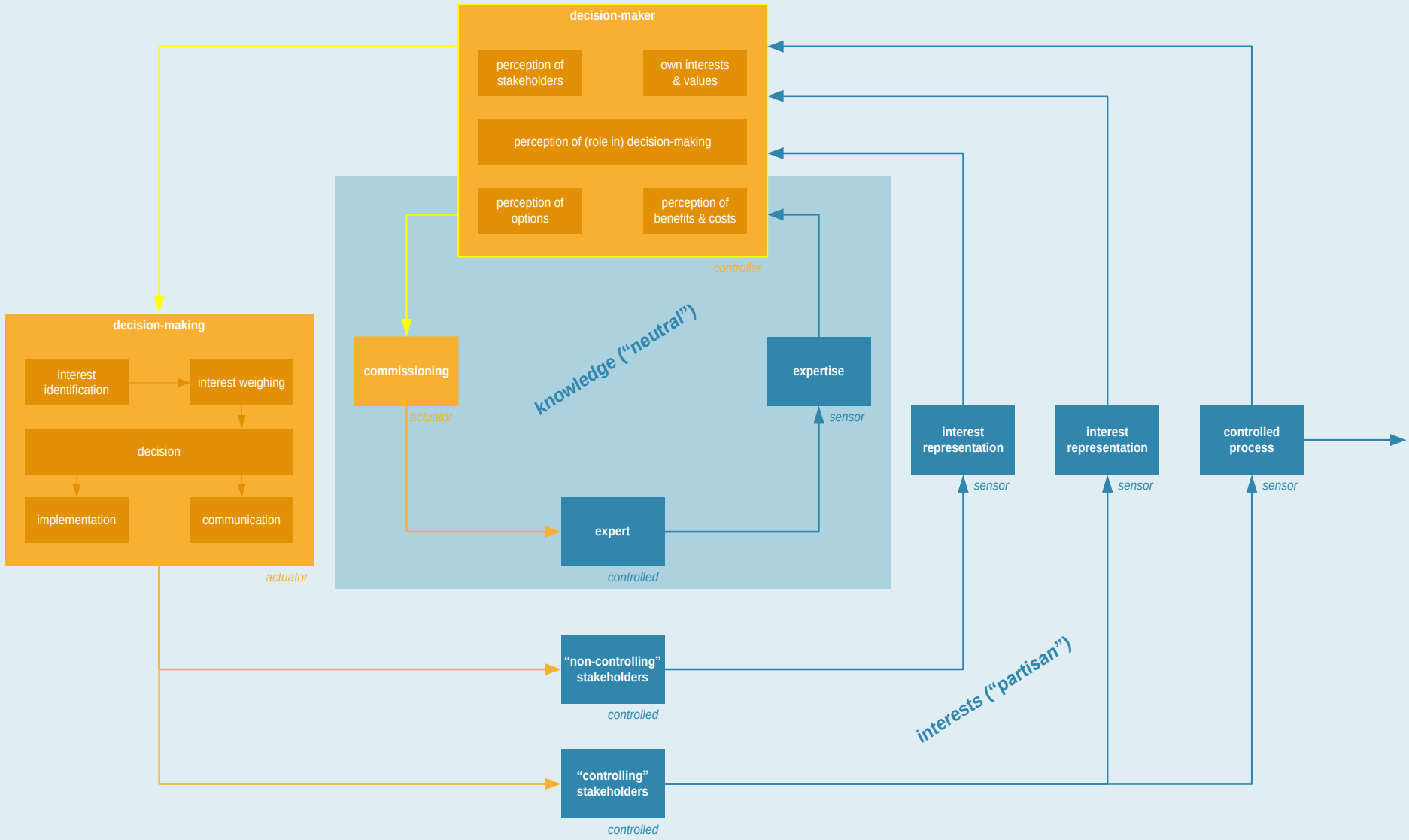
D-STPA: safety constraint + requirement



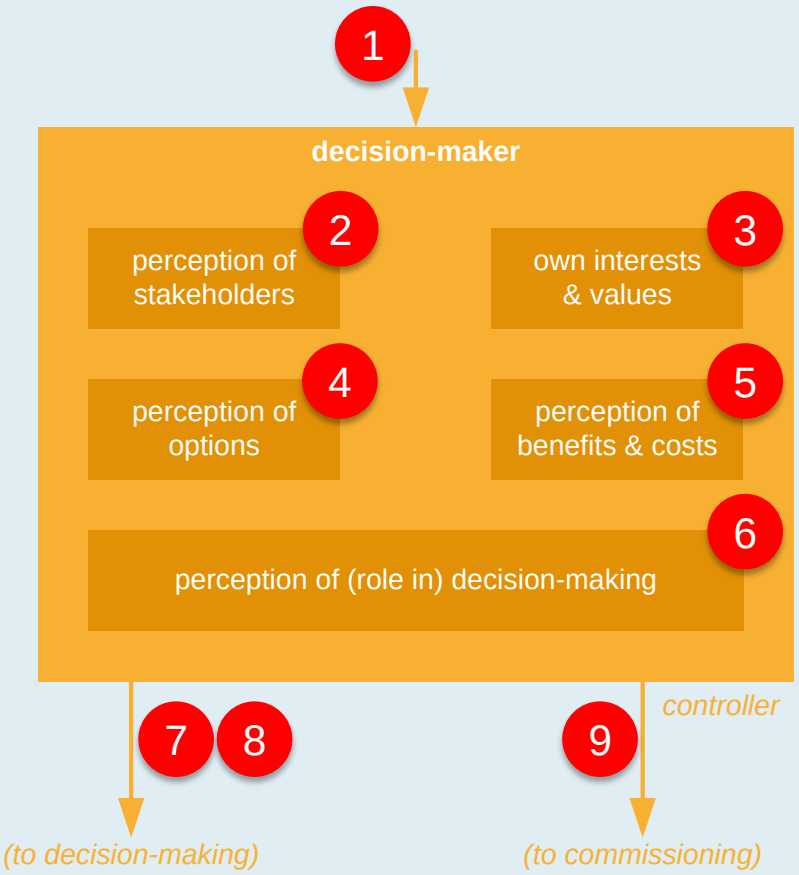
Potential control flaws

- STPA provides powerful means to localize and understand potential control flaws
- Control flaws are generic
- D-STPA aims to do the same
- 36 potential control flaws identified

Controller-related flaws

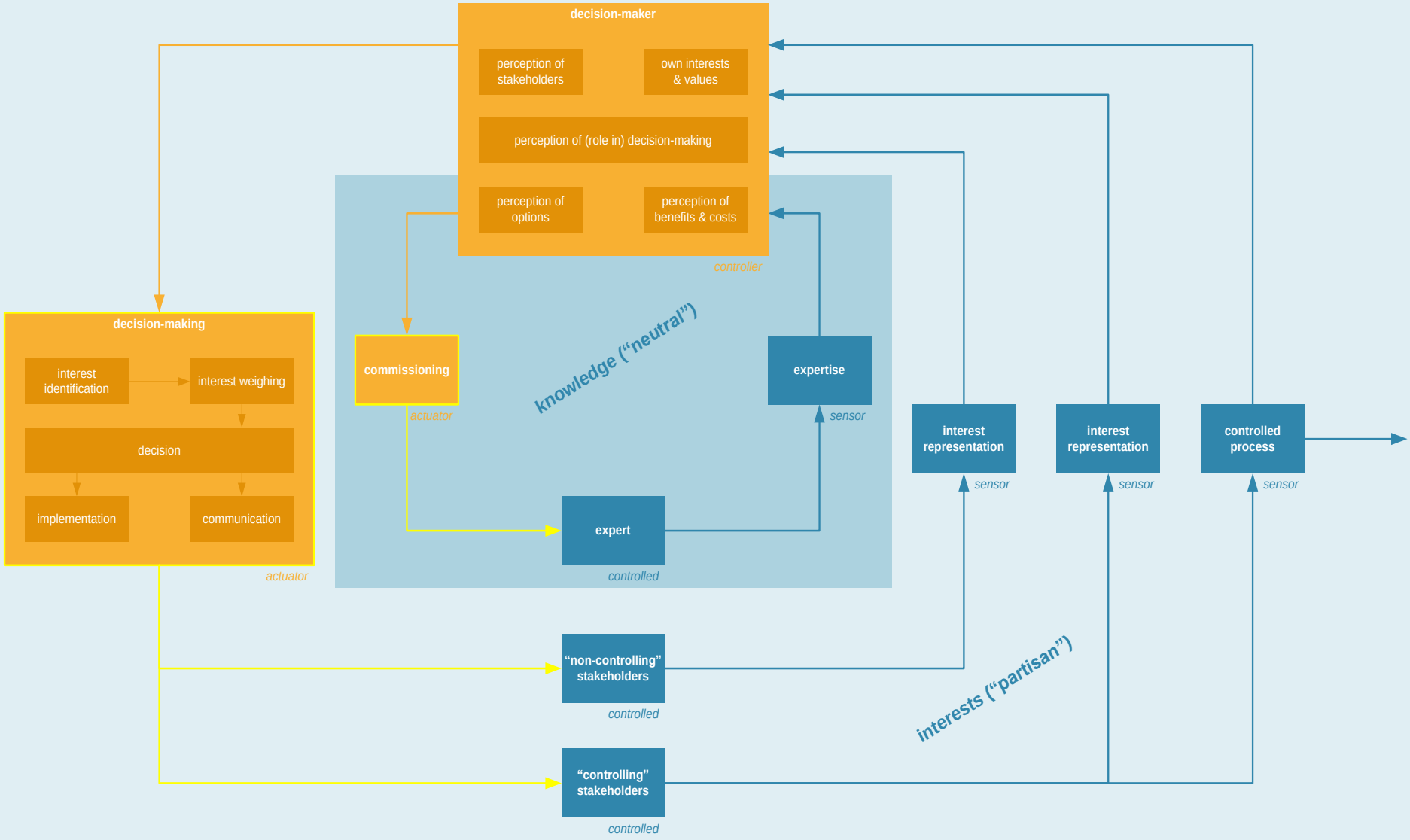


Controller-related flaws

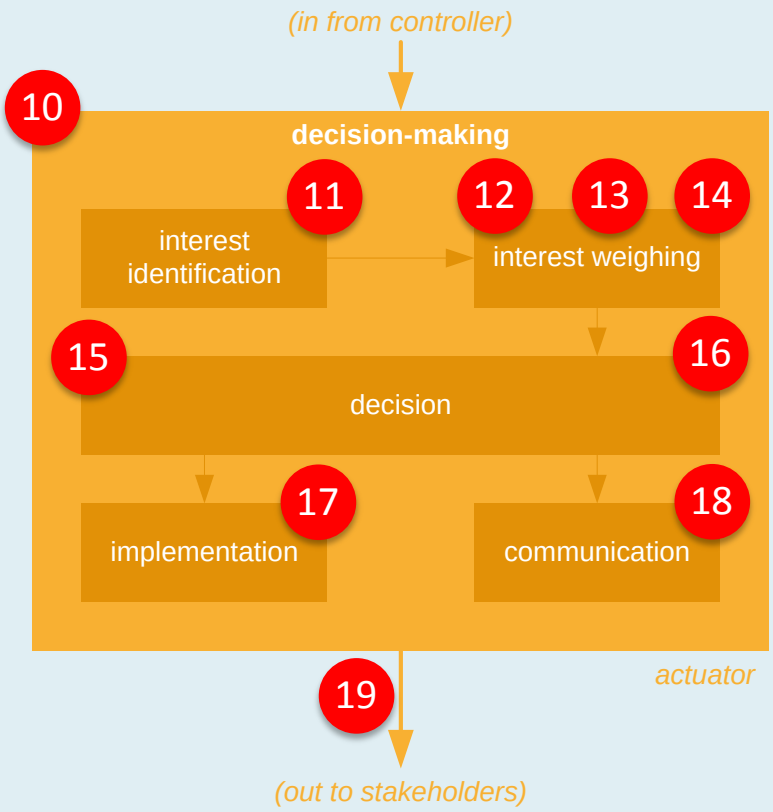


#	Description	Corresponding STPA category
1	external influence (new insights, sudden developments, etc.)	input wrong / missing
2	predisposition towards stakeholders affects decision-making	context
3	DM's own interests unduly affect decision-making	context
4	options available remain unexplored	process model flaws
5	flawed understanding of costs / benefits	process model flaws
6	flawed understanding of own role in decision-making	control algorithm flaws
7	no authority to make decision	control action flaws
8	decision-making starts late or not at all	control action flaws
9	no authority / budget to commission research	control action flaws

Actuator-related flaws

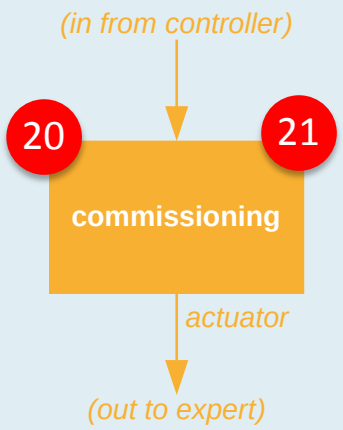


Actuator-related flaws



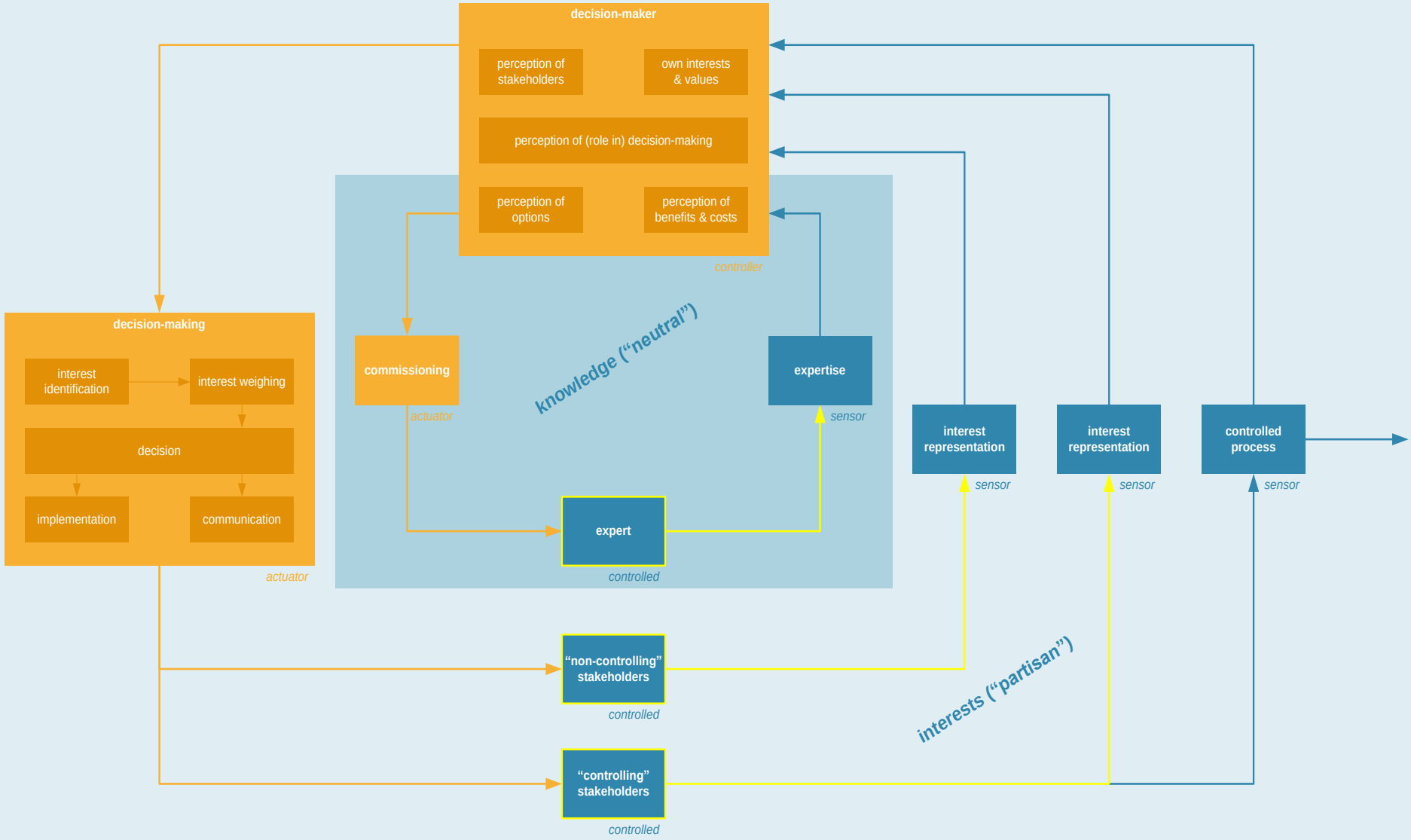
#	Description	Corresponding STPA category
10	time pressure affects decision-making	context
11	interest identification incomplete / biased	inadequate operation
12	frame of reference for interest weighing missing or flawed	inadequate operation
13	arguments disregarded, dismissed, under- or overvalued	inadequate operation
14	dominance of vested interests / desire to maintain status quo	inadequate operation
15	decision too vague, unlawful or impracticable	inadequate operation
16	decision contributes to system hazard	contribution to system hazard
17	flaws in implementation	inadequate operation
18	flaws in communication	inadequate operation
19	time delays, esp. in communication	delayed operation

Actuator-related flaws

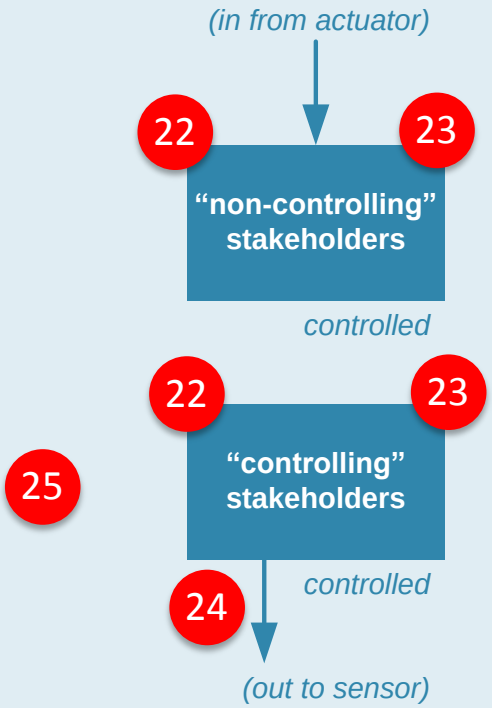


#	Description	Corresponding STPA category
20	commission unspecific / biased towards particular outcome	inadequate operation
21	allocated time and budget restrict thoroughness of research	inadequate operation

Controlled-related flaws

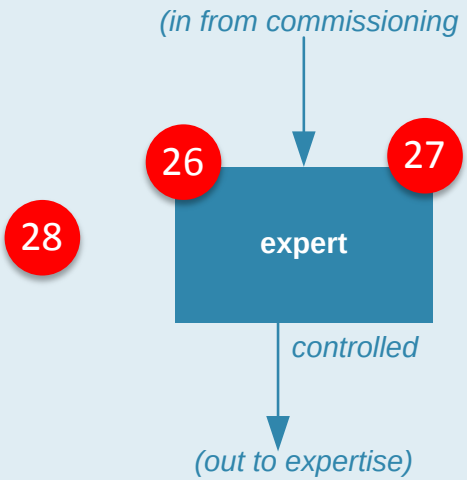


Controlled-related flaws



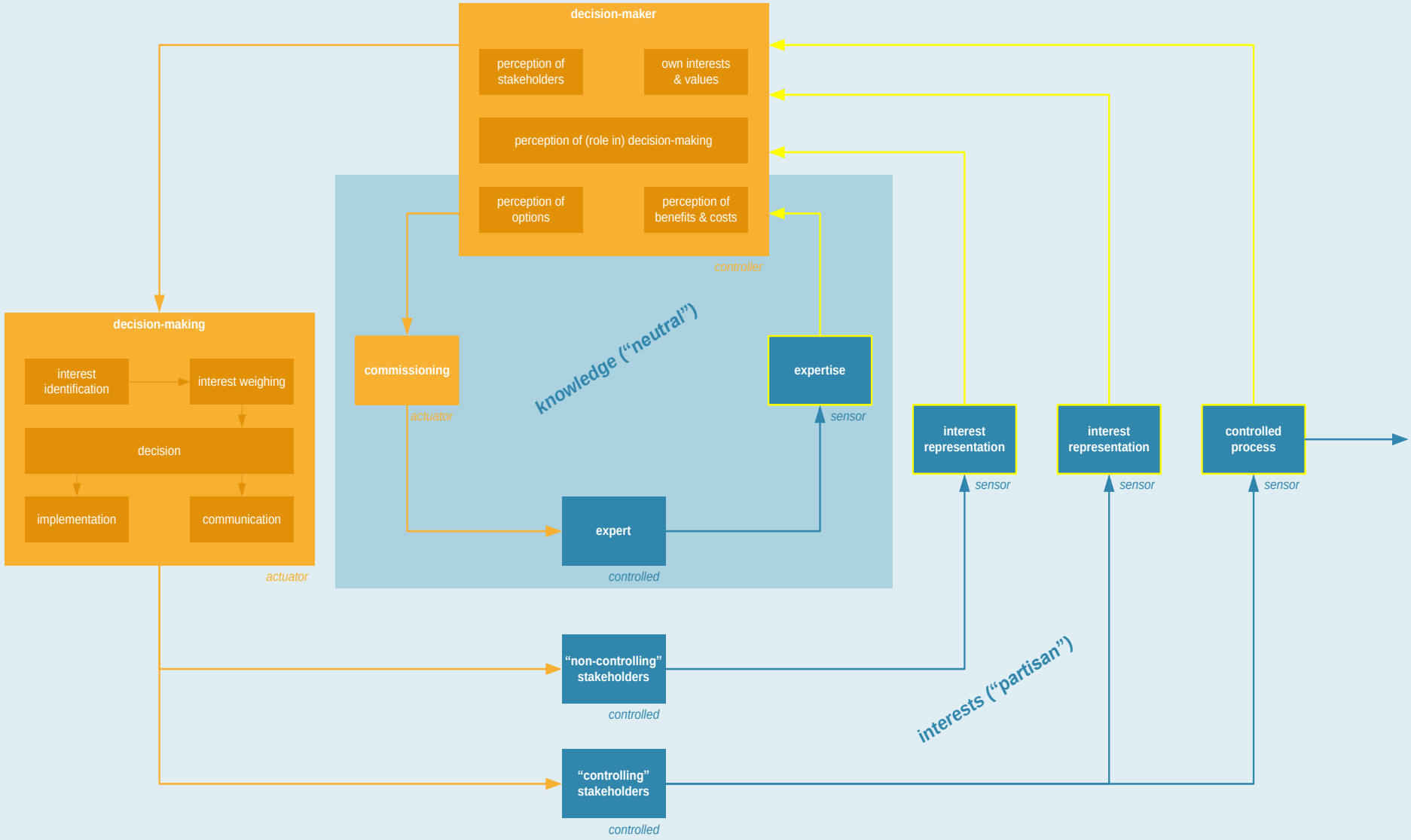
#	Description	Corresponding STPA category
22	stakeholder unaware of impending decision and/or need to represent his interests	control algorithm flaw?
23	stakeholder misunderstands or miscalculates his rights and/or position in the decision-making process	process model flaw
24	stakeholder unable to organize interest representation, or too late	control action flaw
25	external forces prompt stakeholder to ignore decision	out-of-range disturbance

Controlled-related flaws

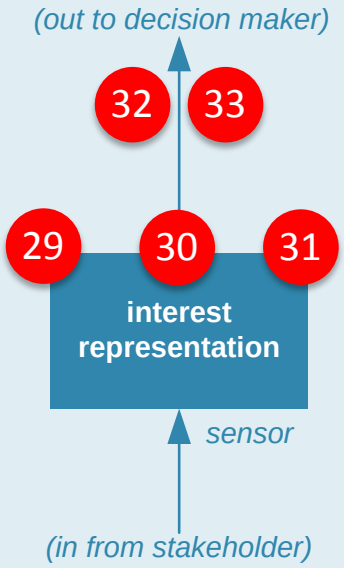


#	Description	Corresponding STPA category
26	experts anticipate DM's expectations of research	component failure?
27	expert's knowledge is outdated	changes over time
28	experts vulnerable to external influence (for instance, by stakeholders)	out-of-range disturbance

Sensor-related flaws

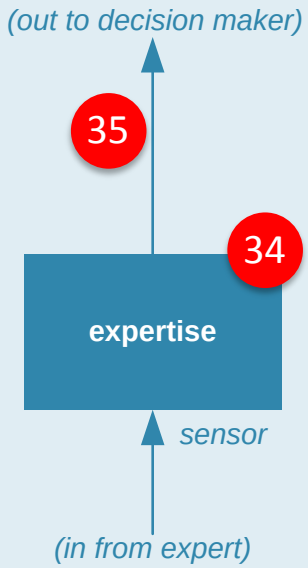


Sensor-related flaws



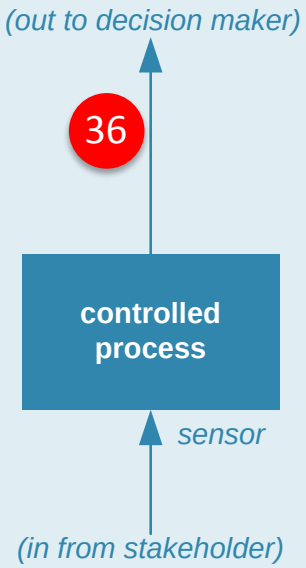
#	Description	Corresponding STPA category
29	costs are overstated and/or benefits played down	inadequate operation
30	interest representation targets actor other than DM	inadequate operation
31	stakeholder lacks information necessary for interest representation	inadequate operation
32	access to DM is denied / impeded	inadequate feedback
33	interests aren't voiced clearly / interest representation does not follow DM's train of thought	inadequate feedback

Sensor-related flaws



#	Description	Corresponding STPA category
34	research is flawed or fraudulous	inadequate operation
35	DM misinterprets / ignores outcomes of research	inadequate feedback

Sensor-related flaws



#	Description	Corresponding STPA category
36	Undesired effects of earlier decisions take too long to become visible	feedback delays

Conclusion

D-STPA enables systematic investigation into
many types of decision-making,
thereby improving our understanding of
how decision-making may impact on safety

Where from here?

- Apply in actual investigation (planned)
- Improve theoretical underpinning (governance literature)
- Further improve D-STPA to include other decision-making configurations
- If possible, reduce complexity (esp. the number of potential control flaws)
- Apply consistenly in all investigations -> build up a catalogue of high-level control structures and corresponding flaws

DUTCH
SAFETY BOARD

Questions?

n.smit@safetyboard.nl