STPA Applied to New Satellite Development and Lessons Learned

Keisuke Sugawara
Naoki Ishihama
Masafumi Katahira

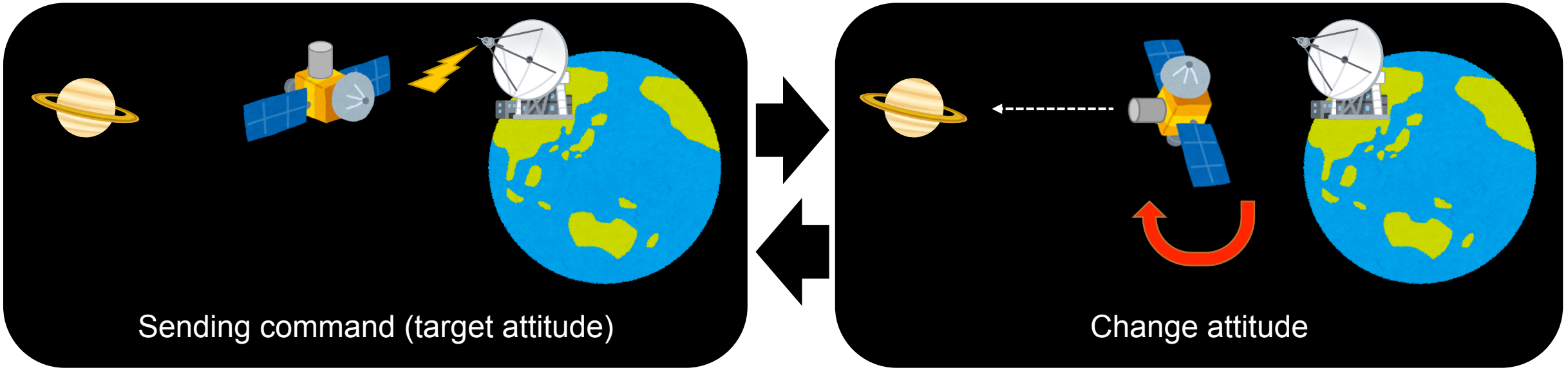
Japan Aerospace eXploration Agency
Research and Development Directorate

Outline

- Background:
  - Mission and Safety of Satellite
  - Requirement for Attitude control function of satellite
- Applying STAMP/STPA
- Conclusion

Mission and Safety of Satellite

- Mission: Observing points on the ground or astronomical objects.



- Attitude control function has important roles.
  - Pointing to observation target one after another
  - Changing attitude safely
- Difference between systems on the ground (cars, factory, …)
  - Instruments cannot be checked and replaced by human.
  - Satellite must detect faults of equipment, isolate and recover by myself

Requirement for Attitude control function of satellite

Situation where the requirement cannot be met

Achievement of safety

= Keep a satellite sate

Cannot detect faults and continue to observe
[False Negative]

Achievement of mission

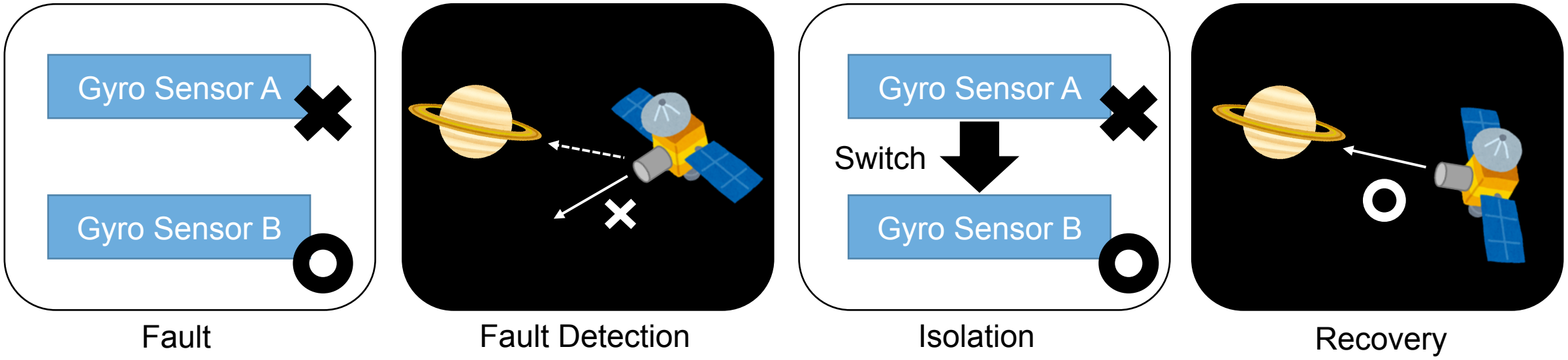
= More observation

False detection and stop to observe
[False Positive]

Necessary and sufficient operation is needed.
Deriving scenarios about the two cases by STAMP/STPA.

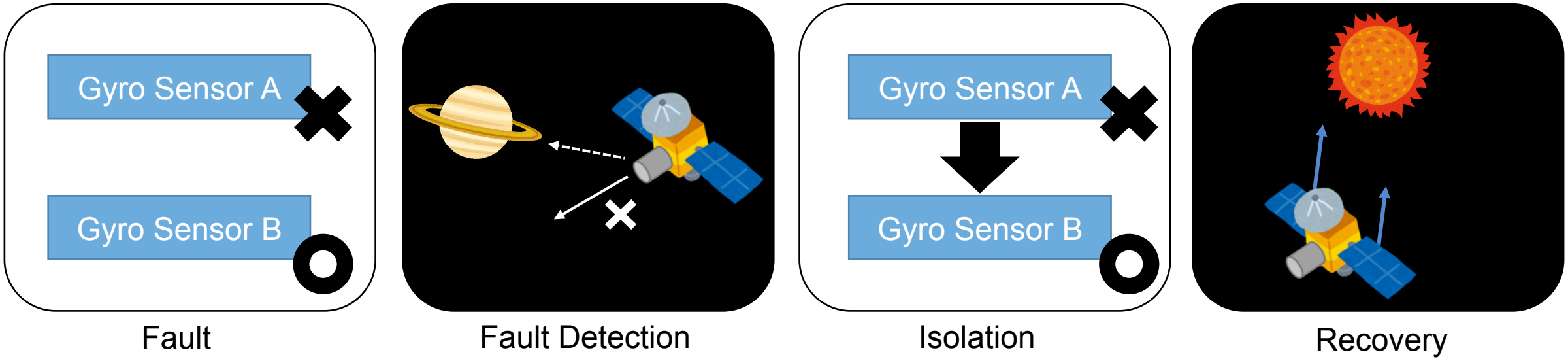
Function for safety of satellite

- Example (1)
  - Fault Detection: Detect deviation between current attitude and target attitude
  - Isolation: Switch to redundant system
  - Recovery: Continue to observe



Function for safety of satellite

- Example (2)
  - Fault Detection: Detect deviation between current attitude and target attitude
  - Isolation: Switch to redundant system, stop observation
  - Recovery: Change attitude to the sun and secure energy from the sun



How to apply STAMP/STPA?

1) Define Purpose of the analysis

2) Model the Control Structure Diagram

3) Identify Unsafe Control Actions

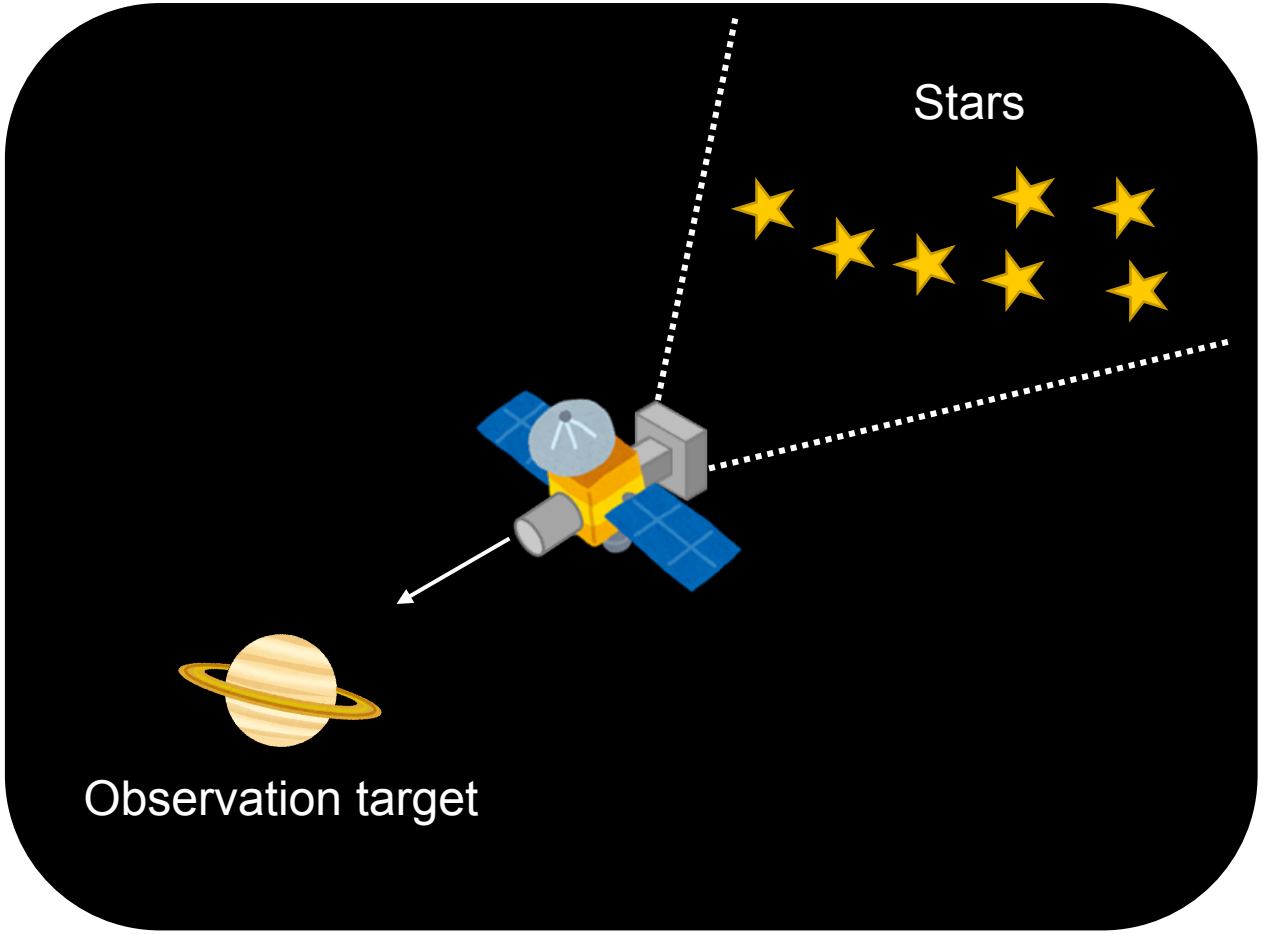
4) Identify Loss Scenarios

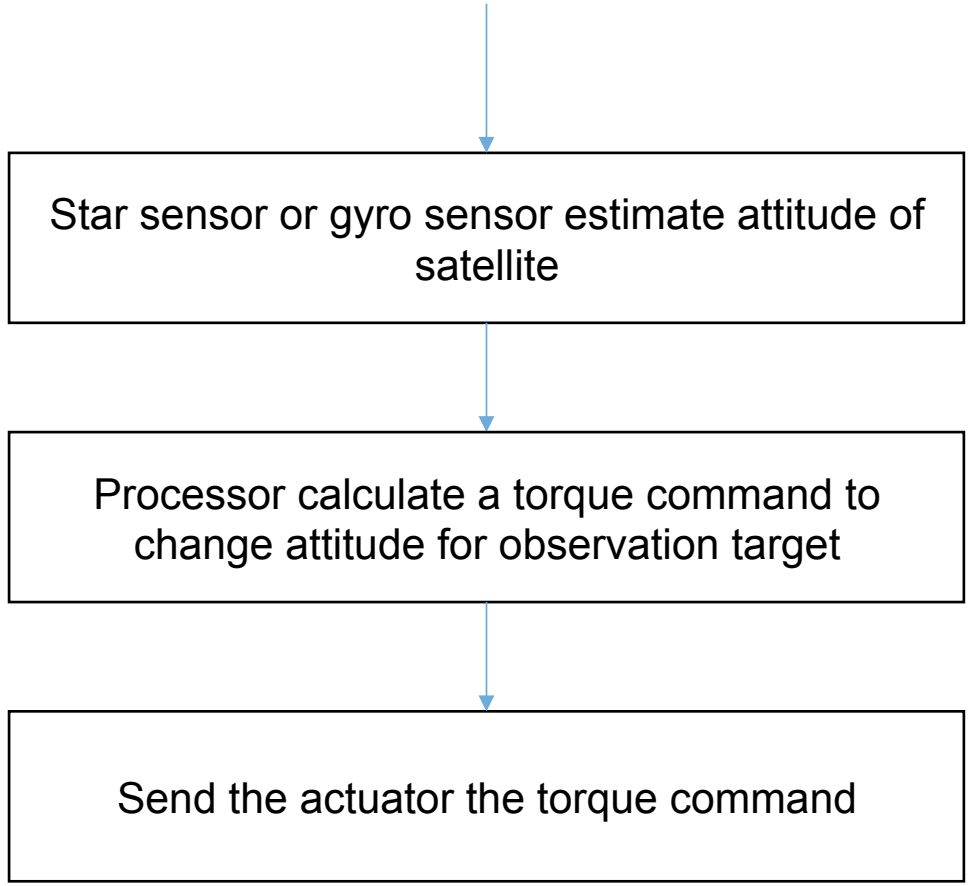
Identify Safety Constraints

Consider concrete design (component, software…) of satellite

Design to keep within the Safety Constraints

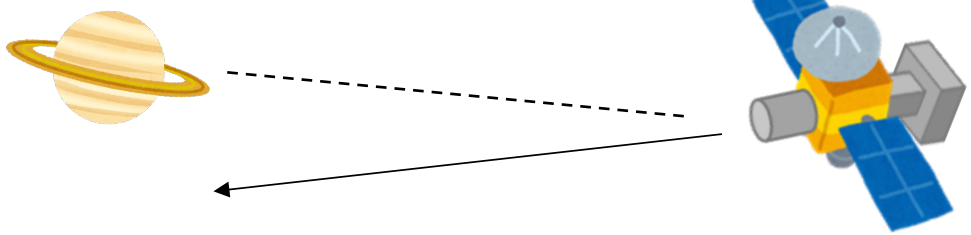
Attitude control subsystem of satellite





Sequence of attitude control (Example)

Attitude control subsystem of satellite



Satellite cannot direct to a target

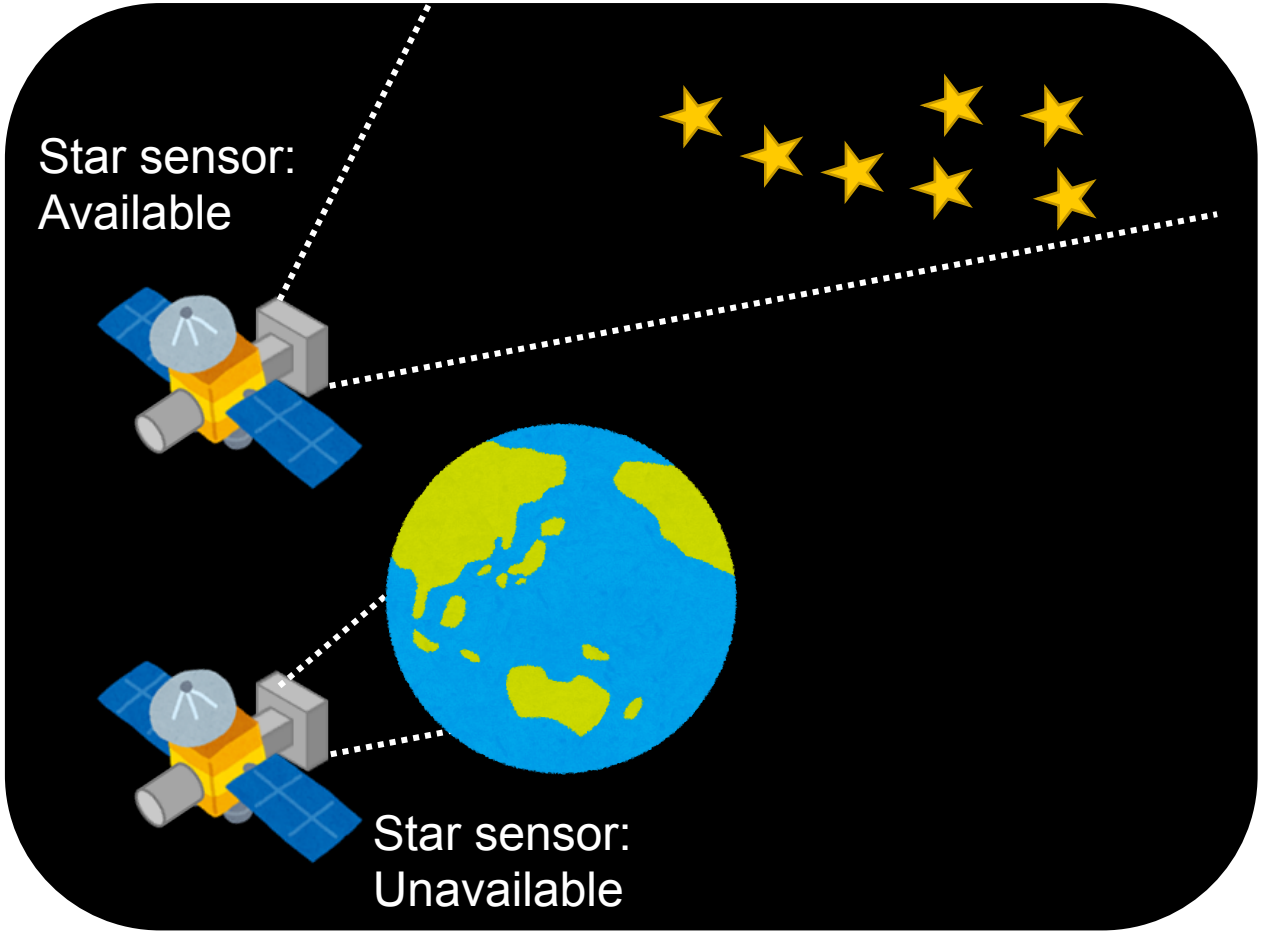
Satellite can be damaged by excessive rotation

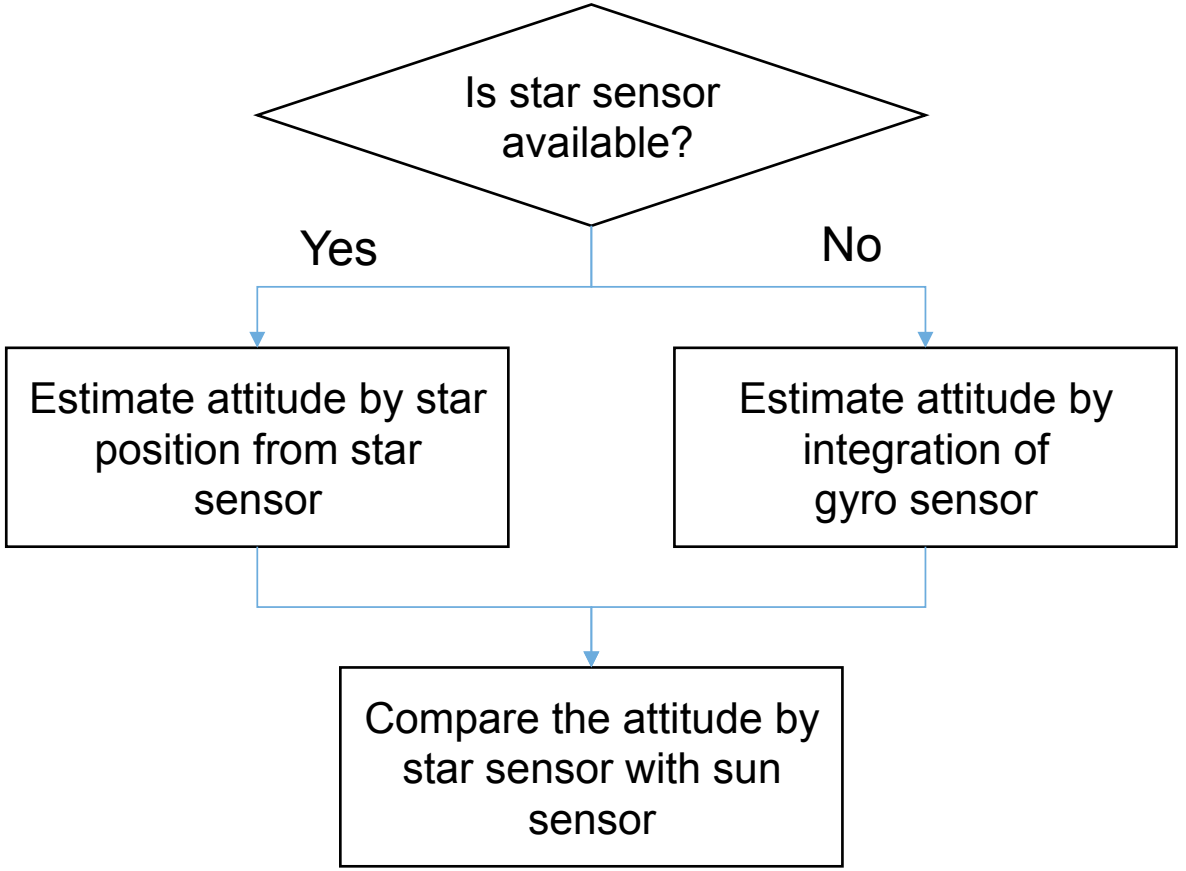
Star sensor or gyro sensor estimate attitude of satellite

Processor calculate a torque command to change attitude for observation target

Send the actuator the torque command

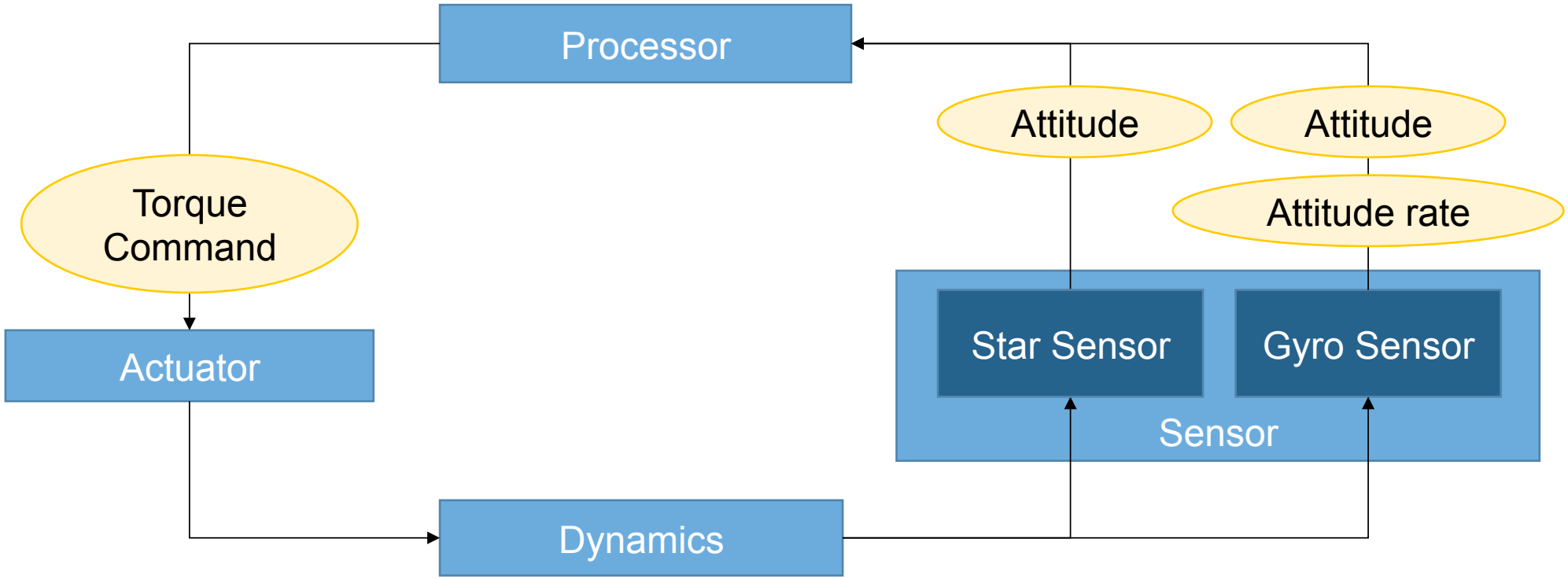
Attitude control subsystem (Estimate attitude)





Sequence of attitude control (Example)

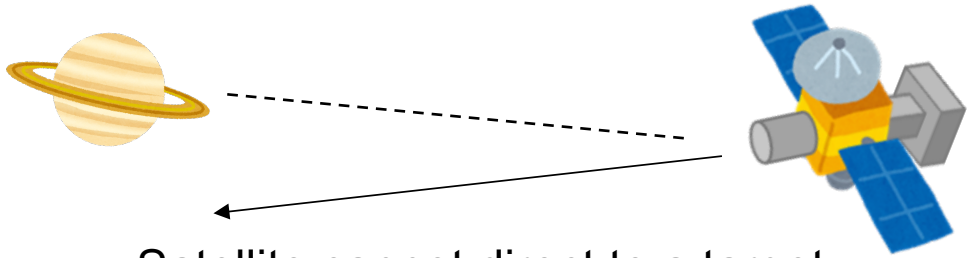
Control Structure Diagram



Torque commands from processor to actuator are most important and can be critical in terms of control.

Unsafe Control Actions

	Not Providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, Applied too long
Torque Command	**UCA-1:** **The processor does not give a torque command for observation target.**	**UCA-2:** **The processor gives a larger torque command than expected.** **UCA-3:** **The Processor gives smaller torque command than expected.**	UCA-4: The processor's torque command to the observation target is delayed.	UCA-5: The torque command for observation target is interrupted. UCA-6: The torque command for observation target dose not stop.

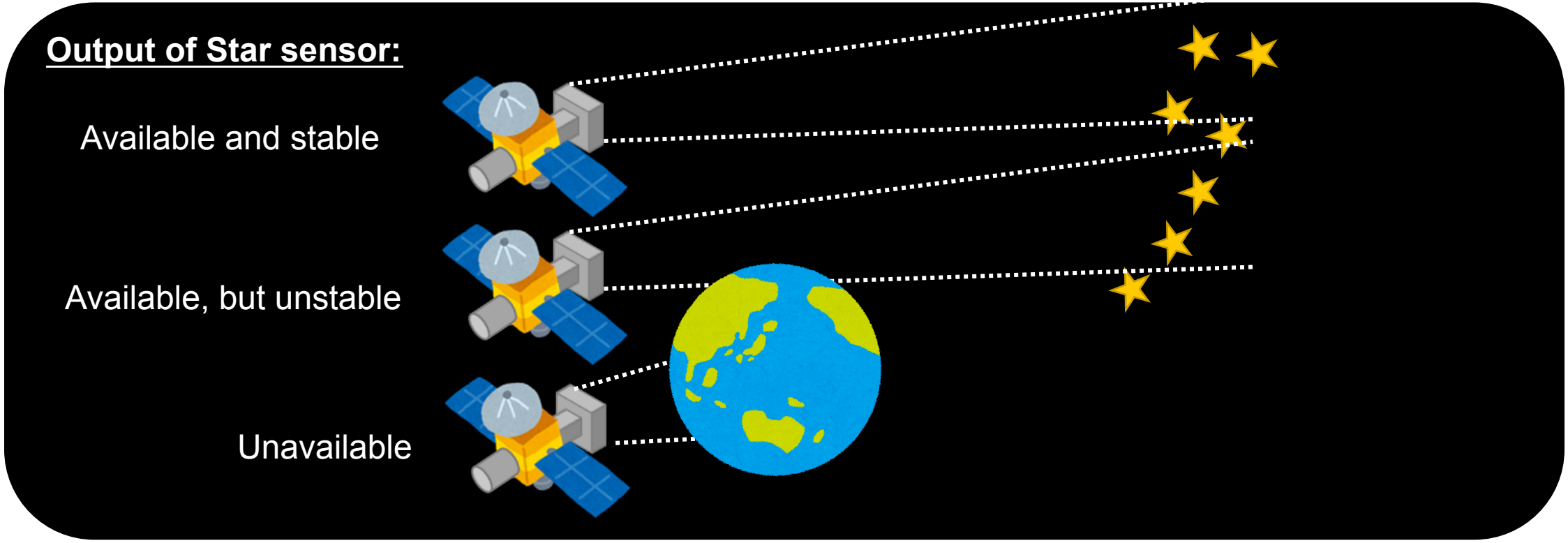


Satellite cannot direct to a target

Satellite can be damaged by excessive rotation

Hazard Scenarios

	Scenario Types	Basic Scenarios	Refine Scenarios
UCA-2: The processor gives a larger torque command than expected.	Inappropriate Decisions	It is judged that a sensor output is stable although actually unstable.	When star sensor is transient state and output is unstable, processor misrecognizes current attitude.



Safety Constraints

Identify Loss Scenarios

When star sensor is transient state and output is unstable, processor misrecognizes current attitude.

Identify Safety Constraints

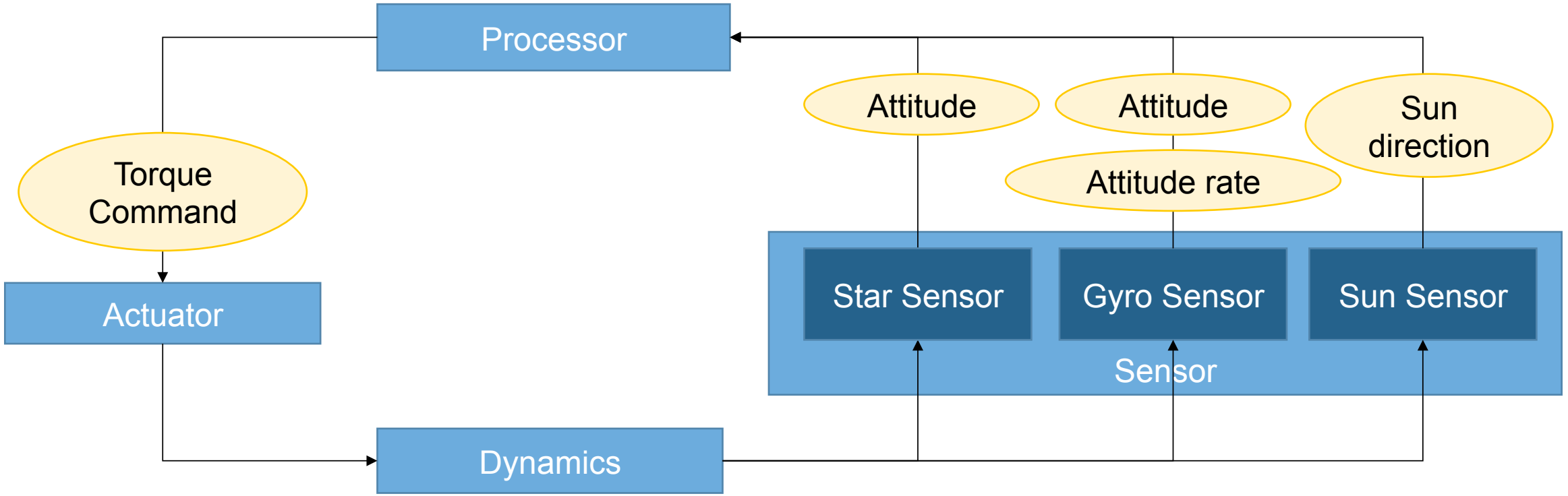
Processor must know that star sensor is transient state or not.

Designing plan (depends on components that satellite has)

[Case 1] If satellite has another sensor such as sun sensor.
→ Compare output of star sensor with output of sun sensor.
If they are different, star sensor is not be used.

[Case 2] Measures by software.
→ Judge current state of star sensor (transient or not) by software.
If transient, use gyro sensor to estimate attitude.

Control Structure Diagram



Torque commands from processor to actuator are most important and can be critical in terms of control.

Conclusion

- Requirement for Attitude control subsystem
  - Achievement of safety
  - Achievement of mission
- Necessary and sufficient operation is needed.

- Following STAMP/STPA framework, we identified constraints on the satellite's attitude control function.
- Identifying Safety Constraints is versatile method for general satellite.
- Concrete design for safety is determined by each satellite.