An Experiment in Modeling Satellite Flight Formation in Event-B

Anton Tarasyuk[1], Inna Pereverzeva[2,3], Elena Troubitsyna[2]

[1] Université de Lorraine & LORIA, Nancy, France

[2] Åbo Akademi University, Turku, Finland

[3] Turku Centre for Computer Science, Turku, Finland

Rodin Workshop, Toulouse

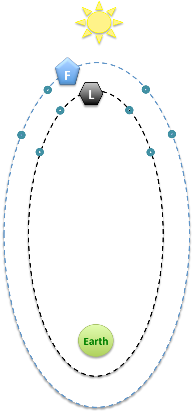
TUCS

Åbo Akademi

Motivation

- Satellite formation flying is the advanced space technology that offers great benefits in acquisition of valuable scientific data
- The **autonomous** aspect significantly complicates the development and verification process
- Testing of the system before deployment is rather unfeasible
- There is a need in rigorous modelling approaches for designing and verifying **inter-satellite coordination mechanisms**
- Work is highly inspired by the PROBA-3 ESA mission (scheduled to be launched in 2017)

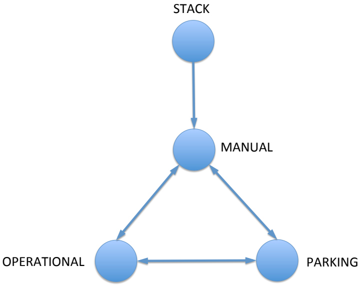
Formation Flying: Description



- The main goal: acquisition of valuable scientific data
- Scientific instruments are distributed over two satellites flying in a formation
  - Main spacecraft (Leader)
  - Companion spacecraft (Follower)
- Spacecraft operate on highly elliptical orbit
  - Formation flying to perform mission objectives at apogee (low gravity region)
  - Formation is periodically broken and reacquired since it cannot be maintained at perigee

Formation Flying: System Modes

We focus on modeling mode transitions (both nominal and off-nominal)

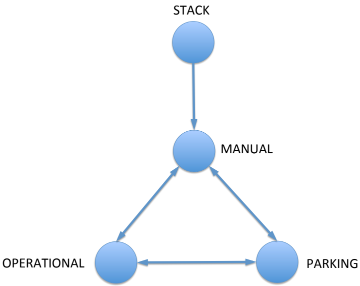


- Mission is organised in four system modes: STACK, MANUAL, OPERATIONAL, PARKING
- STACK is the initial mode; spacecraft are not separated
- MANUAL is the safest mode; used for formation commissioning and in case of problems
- OPERATIONAL and PARKING are "active" modes, where formation flying is performed

TUCS

Åbo Akademi

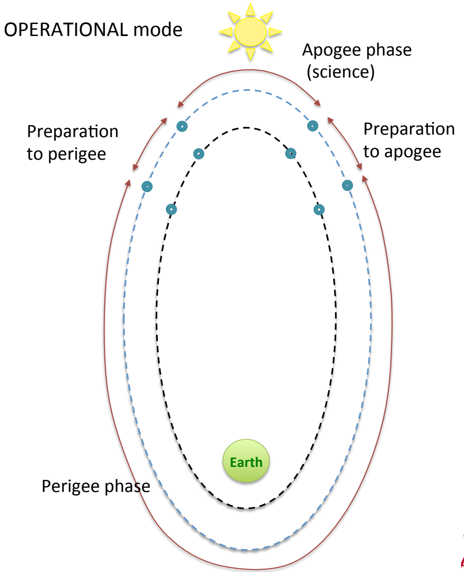
Formation Flying: System Modes (ctd.)



- OPERATIONAL and PARKING modes are rather complex, each consists of a number of sub-modes (phases)
- The phases associated with orbital manoeuvring may consist of a number of sub-phases

Formation Flying: Mode Phases

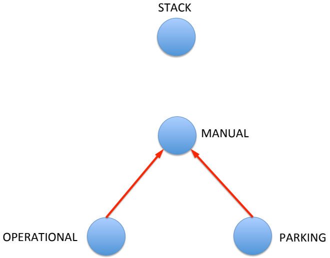
- Preparation to apogee (P1)
- Apogee phase (P2)
- Preparation to perigee (P3)
- Perigee phase (P4)



Communication

- The satellites act collaboratively by coordinating their activities via continuous Inter-Satellite Link communication
- The satellites autonomously manage the formation and, in most cases, take mission critical decisions with no ground supervision
- Metrology sensors allow for formation acquisition and relative position determination maintenance
- The Leader spacecraft controls all nominal transitions and performs relative navigation (ensures mode consistency)

Failures



- The off-nominal mode transitions are either controlled by the Leader or preformed independently by each satellite
  - Relative positioning failure: Leader triggers orbital reconfiguration
  - Loss of communication: orbital reconfiguration triggered independently by each satellite
- In both cases the satellites change their modes to MANUAL

Our Approach

- We use Event-B to formally model mode transitions at different system layers
- There are three main sub-systems: two satellites and inter-satellite communication link
  - Failure detection and recovery as well as communication with the ground are also abstractly modelled
  - One can elaborate on these abstract events to model them scrupulously in further refinement steps
- The mode transitions of spacecraft are independent and coordinated only via the communication link
  - The mode consistency requirement is defined via model invariants

Refinement Strategy

- **Abstract model**: focus on the Leader satellite's behaviour (mode transitions)
- **First Refinement**: introduce the Follower satellite
- **Second Refinement**: communication between the satellites (mode-level communication)
- **Third Refinement**: introduce phases and transitions between them, refine communication (phase-level communication)
- **Fourth Refinement**: communication between the satellites and the ground
- **Fifth Refinement**: model decomposition (modularisation)

Abstract Model: Mode Transitions

$$
\begin{array}{l}
\textit{event}\ \textbf{ModeTransition}\ \widehat{=}\\
\textbf{any}\ mode1,\ mode2\\
\quad\textbf{when}\\
\qquad cur\_mode\_leader \neq STACK\\
\qquad failure = FALSE\\
\qquad mode1 \in \{cur\_mode\_leader\} \cup nextMode(cur\_mode\_leader)\\
\qquad mode2 \in \{prev\_mode\_leader, cur\_mode\_leader\}\\
\qquad mode2 = prev\_mode\_leader \Leftrightarrow mode1 = cur\_mode\_leader\\
\quad\textbf{then}\\
\qquad cur\_mode\_leader := mode1\\
\qquad prev\_mode\_leader := mode2\\
\quad\textbf{end}
\end{array}
$$

$$\forall m \cdot m \in MODES \setminus \{STACK\} \Rightarrow nextMode(m) = MODES \setminus \{STACK, m\}$$

$$nextMode(STACK) = \{MANUAL\}$$

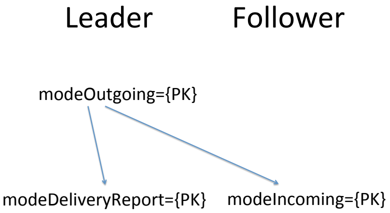
TUCS

Åbo Akademi

Second Refinement: Mode Communication

We introduce three variables to model one-place buffers of the satellites:

- **modeOutgoing** – leader's outgoing buffer
- **modeDeliveryReport** – leader's notification buffer of the delivered command to follower
- **modeIncoming** – follower's incoming buffer



TUCS

Åbo Akademi

Second Refinement: Mode Communication (ctd.)

event **LeaveOperationalMode** $\widehat{=}$
any *mode*
when
$cur\_mode\_leader = OPERATIONAL$
$cur\_mode\_follower = OPERATIONAL$
$failure = FALSE$
$mode \in \{PK, MAN\}$
$modeOutgoing = \varnothing$
...
then
$modeOutgoing := \{mode\}$
end

event **ModeCommunicationLink** $\widehat{=}$
any *msg*
when
$modeOutgoing \neq \varnothing$
$msg \in modeOutgoing \cup \{LOST\}$
then
$modeOutgoing := \varnothing$
$modeDeliveryReport := \{msg\}$
$modeIncoming := \{msg\}$
end

Second Refinement: Mode Communication (ctd.)

- Behaviour of satellites in operational modes is tightly scheduled
  - Fixed duration time of each phase
- Therefore, communication is also scheduled
  - Timers used to identify loss of communication
- Modelling of time is not directly supported by Event-B
  - Better to find a suitable abstraction
- We use delivery of LOST message to abstractly model expired time-outs

Second Refinement: Mode Communication (ctd.)

event **EnterManualModeLeader**
refines **ModeTransitionLeader** $\widehat{=}$
when
$cur\_mode\_leader = OPERATIONAL \lor cur\_mode\_leader = PARKING$
$failure = FALSE$
$modeDeliveryReport = \{MAN\} \lor modeDeliveryReport = \{LOST\} \lor phaseCommFailureL = TRUE$
then
$cur\_mode\_leader := MANUAL$
$prev\_mode\_leader := cur\_mode\_leader$
$modeDeliveryReport := \varnothing$
$phaseCommFailureL := FALSE$
end

Second Refinement: Mode Consistency

$$\mathrm{inv}_1 : cur\_mode\_leader \neq cur\_mode\_follower \Rightarrow$$
$$cur\_mode\_leader = prev\_mode\_follower \vee$$
$$cur\_mode\_follower = prev\_mode\_leader$$

$$\mathrm{inv}_2 : cur\_mode\_leader = cur\_mode\_follower \Rightarrow$$
$$prev\_mode\_leader = prev\_mode\_follower$$

$$\mathrm{inv}_3 : modeOutgoing \neq \varnothing \Rightarrow cur\_mode\_leader = cur\_mode\_follower$$

TUCS

Åbo Akademi

Second Refinement: Formation Failure

- We also model possibility of **formation (position) failure** – potential danger of satellites collision
- In that case, Leader commands transition to MANUAL mode (pre-defined safe orbits, no other manoeuvres are allowed)

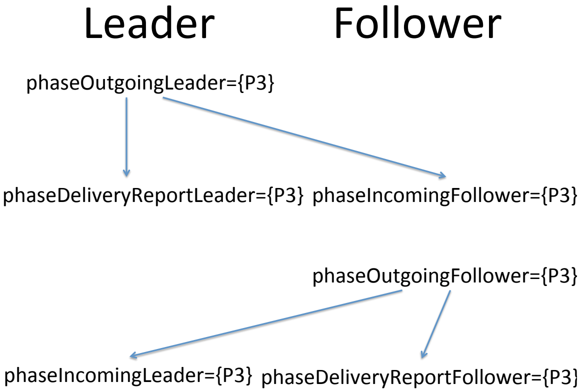
event **FormationFailureReaction** $\widehat{=}$
when
  $failure = TRUE$
  $\ldots$
then
  $modeOutgoing := \{MAN\}$
end

Third Refinement: Phase Communication

To model a phase-level communication we introduce six variables to model one-place buffers of the satellites:

- **phaseOutgoingLeader** – leader's outgoing buffer
- **phaseIncomingLeader** – leader's incoming buffer
- **phaseDeliveryReportLeader** – leader's notification buffer
- **phaseOutgoingFollower** – follower's outgoing buffer
- **phaseIncomingFollowe** – follower's incoming buffer
- **phaseDeliveryReportFollower** – follower's notification buffer

Third Refinement: Phase Communication (Ctd.)



TUCS

Åbo Akademi

Third Refinement: Phase Communication (Ctd.)

event **LeavePhase2** $\widehat{=}$
when
$cur\_phase\_leader = PHASE2$
$failure = FALSE$
$modeDeliveryReport = \varnothing$
$phaseOutgoingLeader = \varnothing$
$phaseIncomingLeader = \{P2\}$
$phaseDeliveryReportLeader = \varnothing$
then
$phaseOutgoingLeader := \{P3\}$
$phaseIncomingLeader := \varnothing$
end

event **EnterPhase3Follower** $\widehat{=}$
when
$cur\_phase\_follower = PHASE2$
$modeIncoming = \varnothing$
$phaseOutgoingFollower = \varnothing$
$phaseIncomingFollower = \{P3\}$
then
$phaseIncomingFollower := \varnothing$
$cur\_phase\_follower := PHASE3$
$prev\_phase\_follower := cur\_phase\_follower$
$phaseOutgoingFollower := \{P3\}$
$phaseDeliveryReportFollower := \varnothing$
end

Fifth Refinement: Decomposition

- The use of modularisation plug-in to Event-B (in progress)
- Separate interfaces for Leader, Follower and Ground Control
- The interface for the follower satellite can be potentially implemented multiple times to model larger formations
  - In this case redevelopment of the leader satellite is inevitable
  - Approach to model communication can be reused with small changes

Wrapping Up

- Very interesting case study to work on
- Despite seeming simplicity of the model and mode consistency invariants, the proving effort was pretty significant (required us to define a substantial number of additional invariants)
- ProB and SMT Solvers plug-ins were of a great help
- Future work:
  - Finalise the model (in particular, decomposition refinement step)
  - Design/refinement patten to enable reuse of communication mechanisms (?)
  - Consider larger formations (?)