WP9: Airborne System Design Requirements
-- Overview

Petr Cásek

iFly Mid Term Review, September 29, 2009

Honeywell

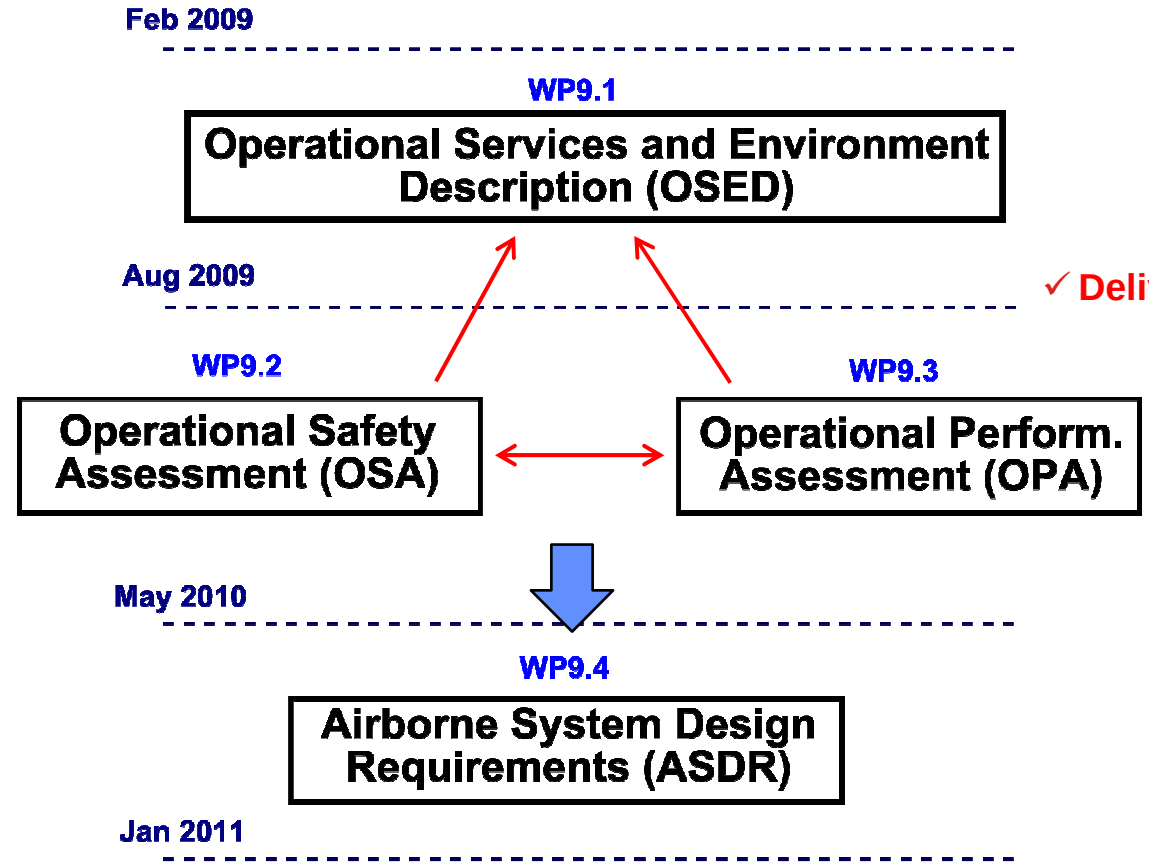
WP 9 Outline

Honeywell

Goal:

Perform a preliminary Safety Performance Requirements (SPR) development cycle according ED78A/DO-264

Schedule & WBS



WP9 Team

Honeywell

Honeywell (leader)

- Petr Cásek: petr.casek@honeywell.com
- Eva Gelnarová: eva.gelnarova@honeywell.com
- Claudia Keinrath: claudia.keinrath@honeywell.com
- Petr Gotthard: petr.gotthard@honeywell.com

Isdefe

- Leticia Biescas Altelarrea: lbiescas@isdefe.es
- Vicente Bordon Galan: vbordon@isdefe.es
- Luis Francisco Burguillo Herrero: lfburguillo@isdefe.es

NLR

- Henk Blom: blom@nlr-atsi.nl
- F.J.L. Bussink: bussinkf@nlr.nl

ENAC

- Stéphane Puechmorel: puechmor@recherche.enac.fr

Dedale

- Amel Sédaoui: asedaoui@dedale.net

University of Tartu

- Aavo Luuk: Aavo.Luuk@ut.ee

EEC

- Richard Irvine: Richard.irvine@eurocontrol.int

Partner	HNWL	Isdefe	NLR	ENAC	UCAM	Dedale	ETHZ	UTartu	EEC	NTUA	Total
WP9.1	**8**	**1**	**0.5**	**0.5**		**0.5**		**0.5**	**0.5**		**11.5**
WP9.2	9	1	0.5		0.5	0.5	0.5	0.5		0.5	**12.5**
WP9.3	8	4	0.5	0.5	0.5		0.5		0.5	0.5	**15.5**
WP9.4	5		0.5	0.5							**6.0**
Total WP9	30	6	2	1.5	1	1	1	1	1	1	**45.5**

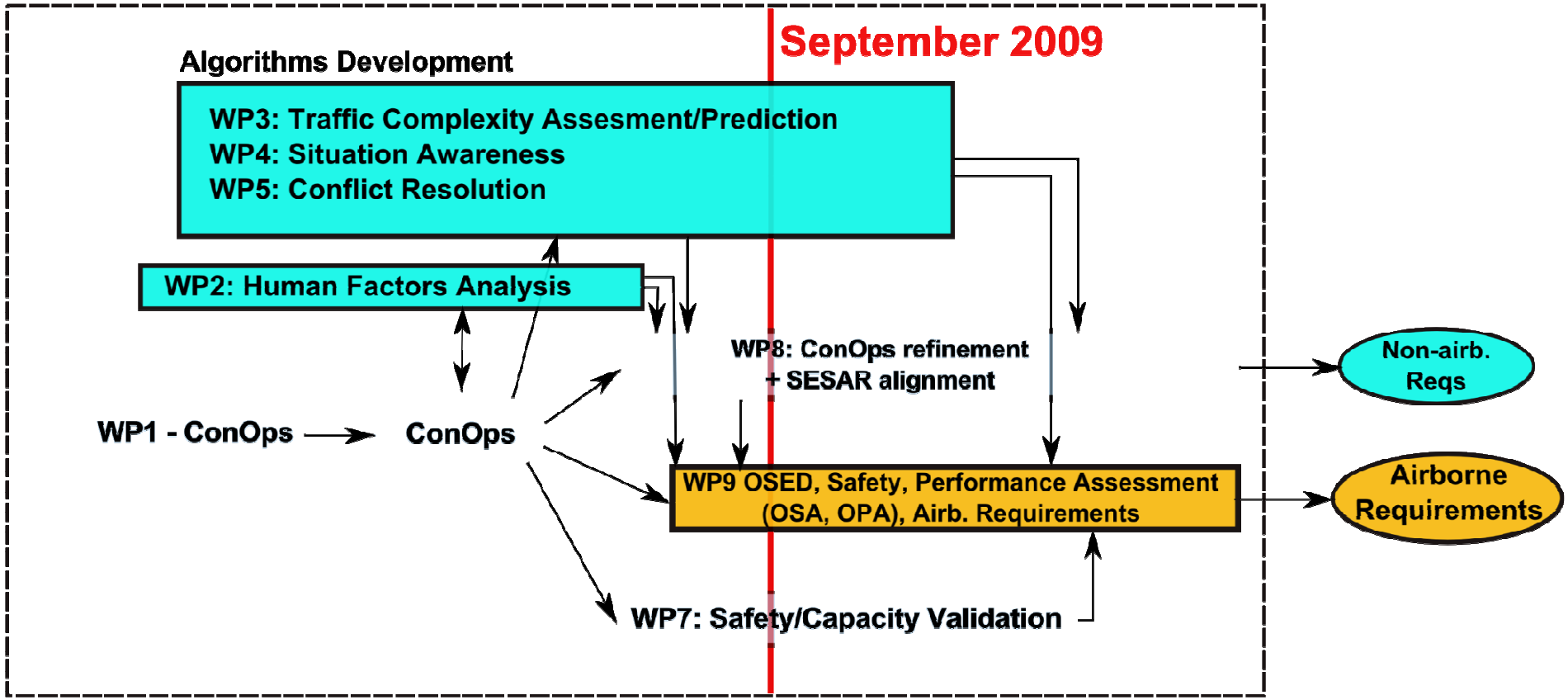
Presentation Outline

Honeywell

- ✓ **WP9.1 – OSED**
  - Considered Inputs
  - Applied Approach
  - OSED Overview
- ➢ **Next/Ongoing steps**
  - Operational Safety Assessment
  - Operational Performance Assessment

WP9 Inputs: Internal within the iFly Project

Honeywell



WP9 Inputs: External

Honeywell

- **Surveillance**
  - MASPS for Aircraft Surveillance Applications DO-289
  - ADS-B MASPS DO-242A
  - 1090 MOPS DO-260A
- **ASAS**
  - Action Plan 23 deliverables D3, D4
  - ASAS MOPS DO-317 (Surveillance)
- **ASAS Package I**
  - **ATSA – ITP:** SPR DO-312, NASA HIL Study
  - **ATSA – VSA:** SPR DO-313
  - **ATSA – AIRB/SURF, ASPA-IM:** monitoring evolution of SC-186/WG-51 RFG work on OSED, OSA, OPA documents
- **ACAS**
  - TCAS II high-level documentation
  - TCAS II MOPS DO-185

WP9.1 Approach

Honeywell

Two different views on A3 operations:

Airborne Perspective

- Processing of detected events
- Performance-focused parameterization
- High-level functional system requirements

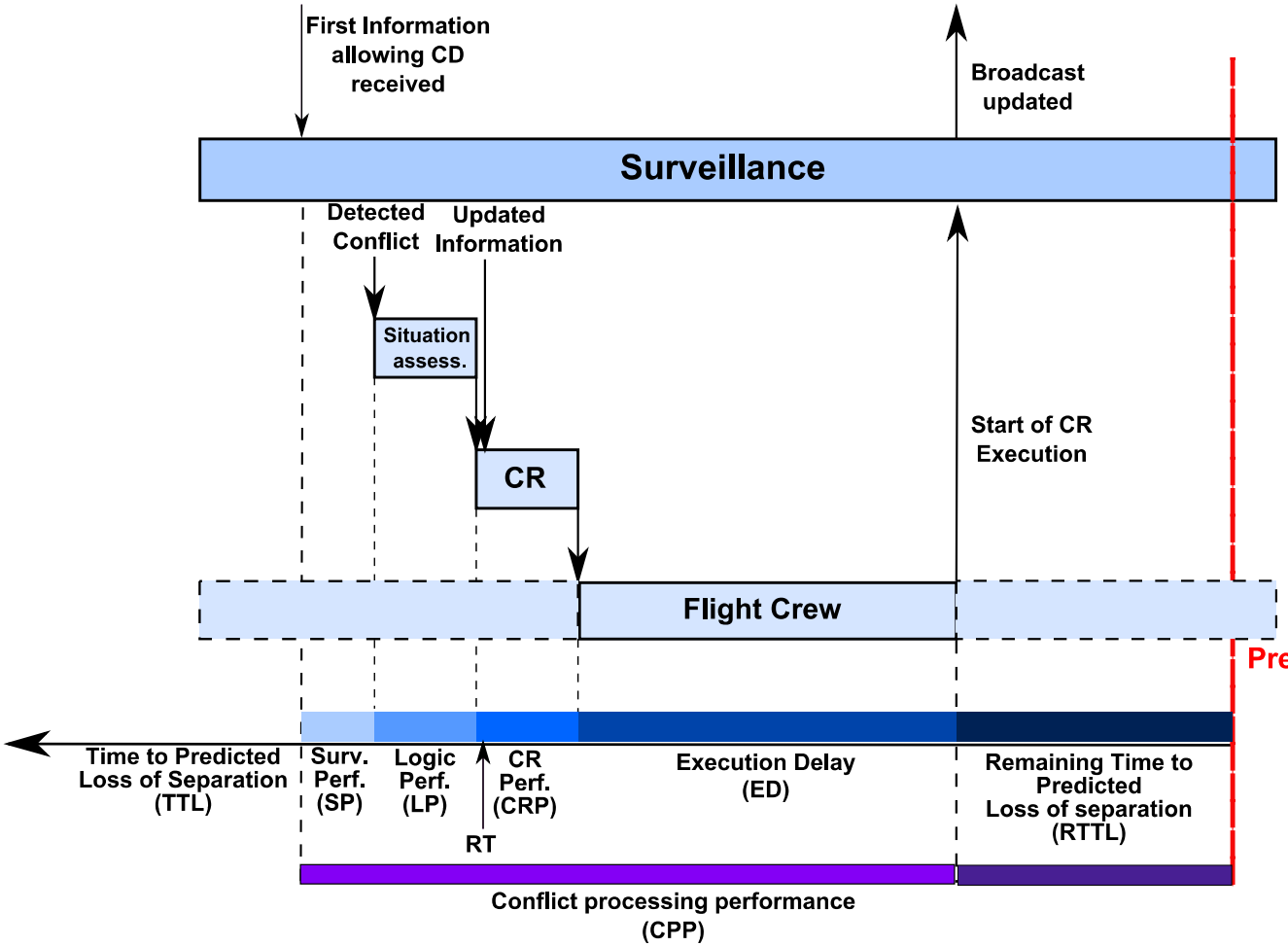
Operational Perspective

- Focus on information (trajectory) sharing
- Decomposition of A3 operations into stages

Airborne View – Conflict Processing

Honeywell

ASAS Separation Management: Reaction to detected threats



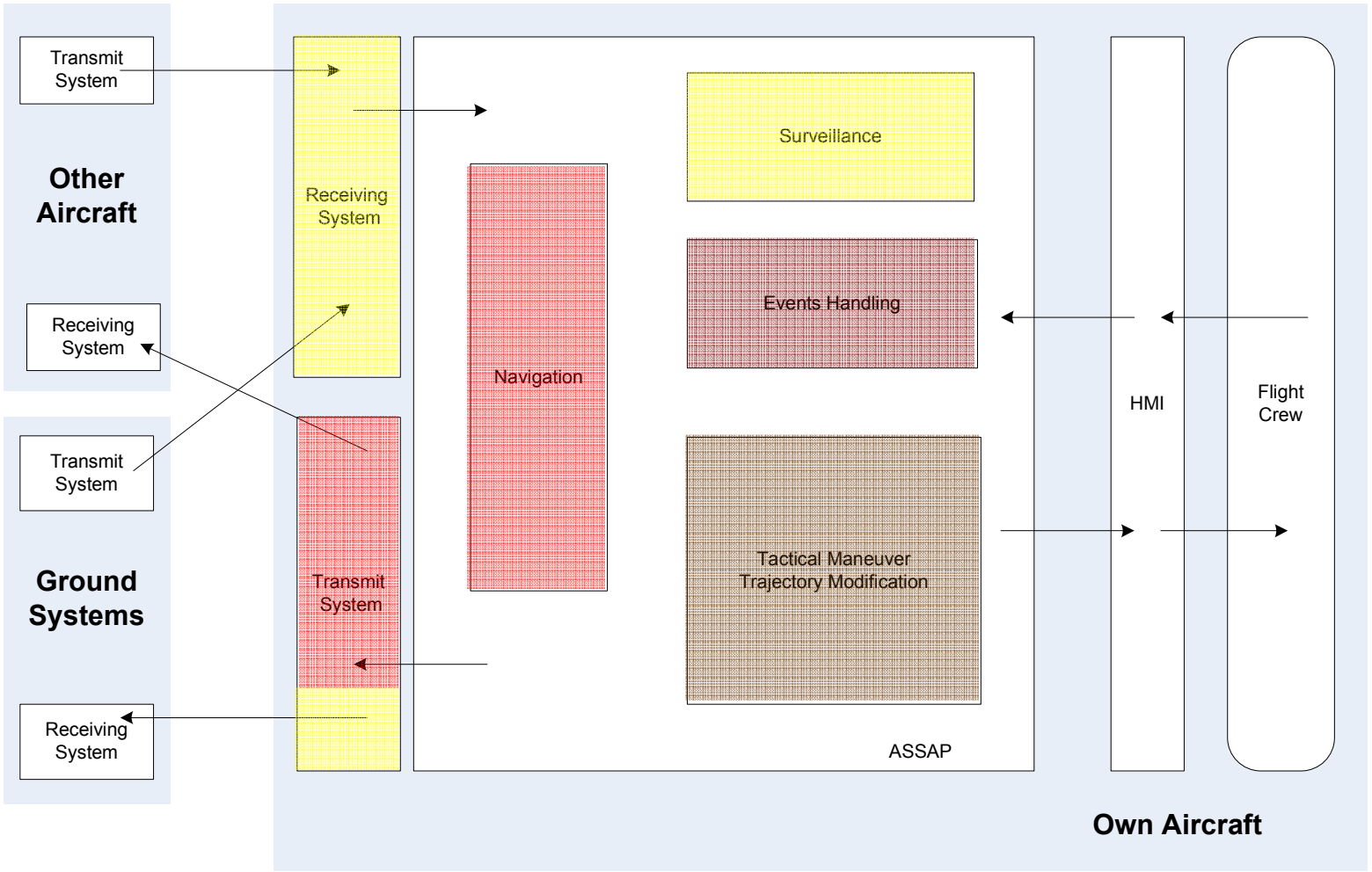
High-level Process Overview

Performance-based Parameterization

Functional Requirements

Honeywell

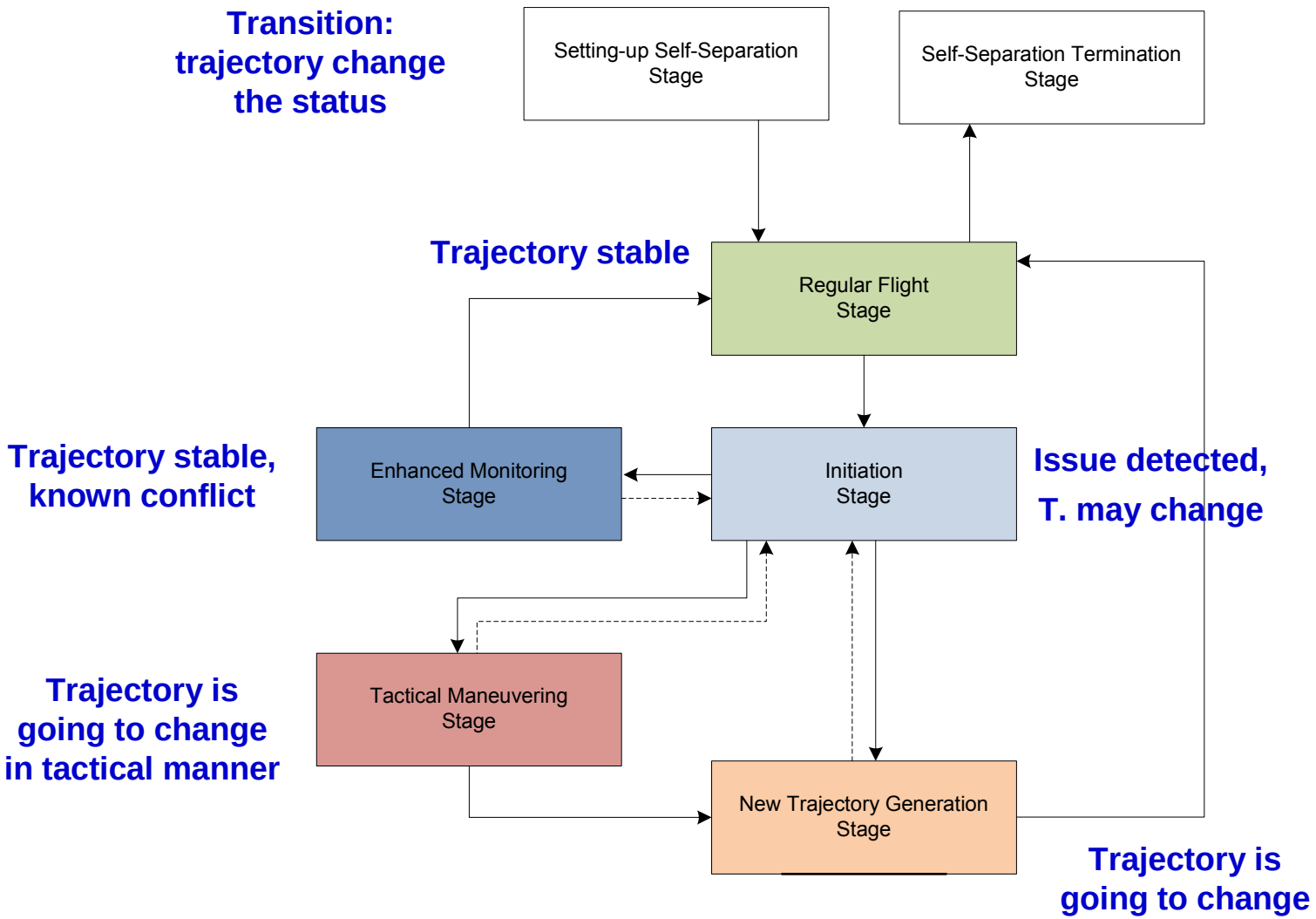
Functional Blocks = a set of related functionalities



Operational View – Decomposition to Stages

Honeywell

Operational perspective: Trajectory status is key.



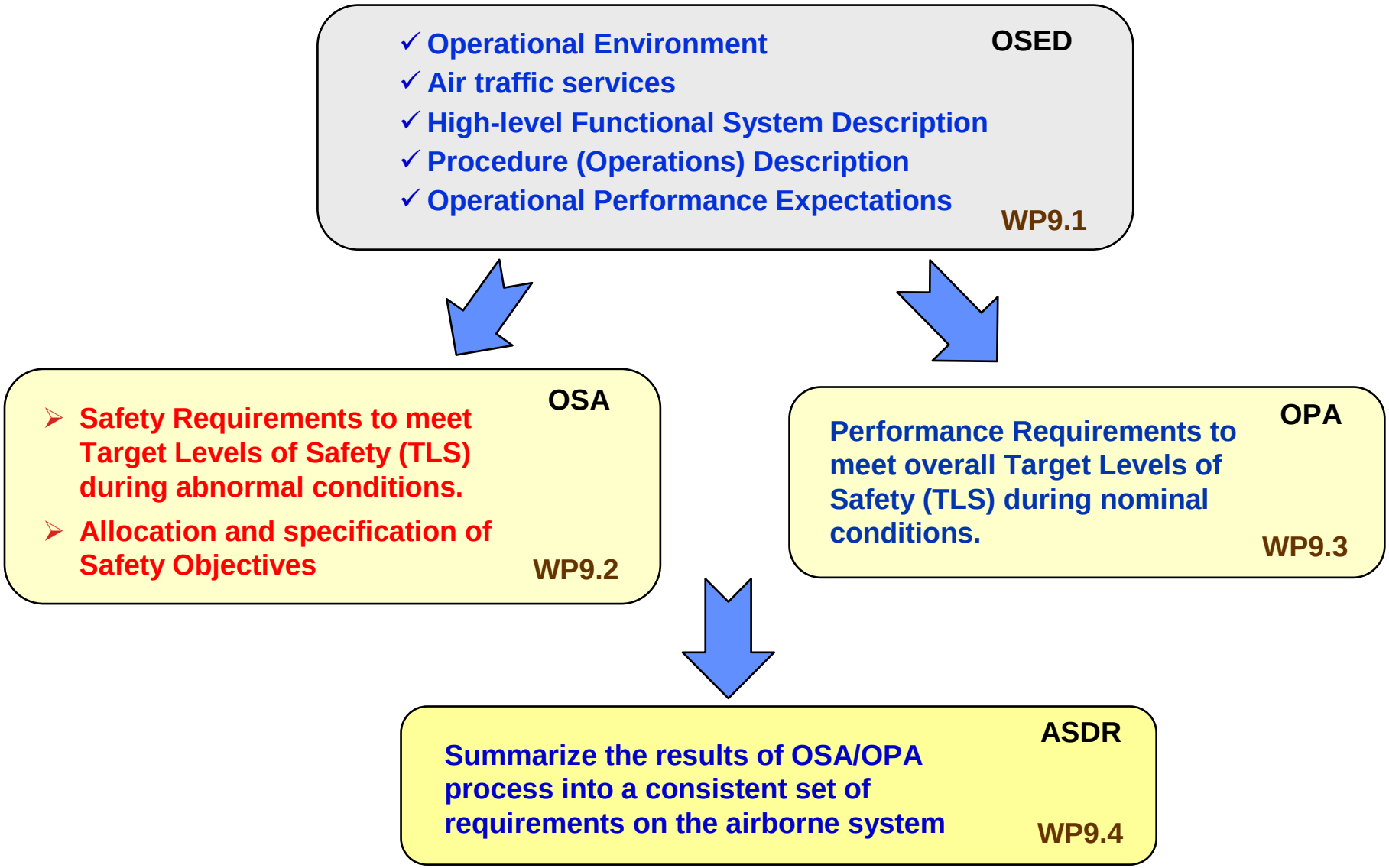
Operational Stages vs. Functional Blocks

Honeywell

Stages	Functional blocks				
	Navigation	Surveillance	Events Handling	Trajectory modification	Tactical maneuver
Regular Flight Stage	X	X			
Initiation Stage	X	X	X		
Enhanced Monitoring Stage	X	X	X		
New Trajectory Generation Stage	X	X	X	X	
Tactical Maneuvering Stage	X	X	X		X

WP9: Next Steps

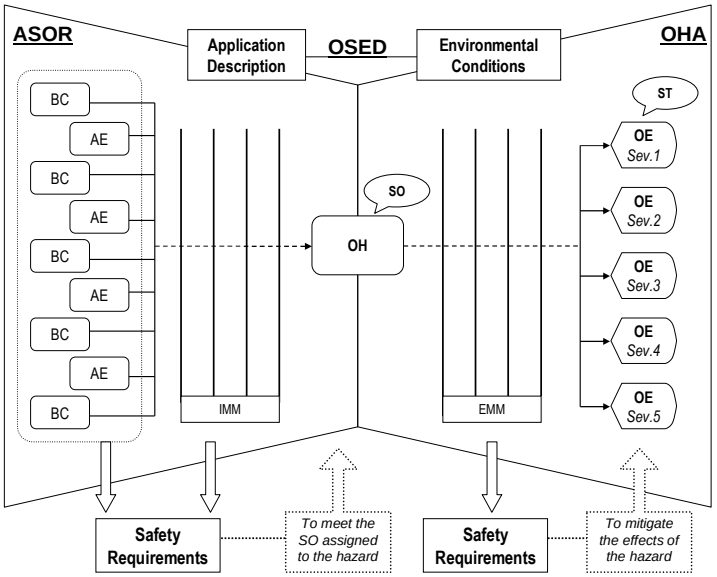
Honeywell



OSA – The Conventional ED-78 Approach

Honeywell

- **Operational Hazard Analysis**
  - Brainstorming sessions (WP7)
  - Expert judgment
- **Event Tree Analysis**
  - External Mitigation Means
  - Equivalent Probability determination
- **Impact classification**
  - Classification of severity
  - TLS specified
- **Fault Tree Analysis**
  - Internal Mitigation Means
  - Allocation of Safety Objectives



OPA – Main Elements

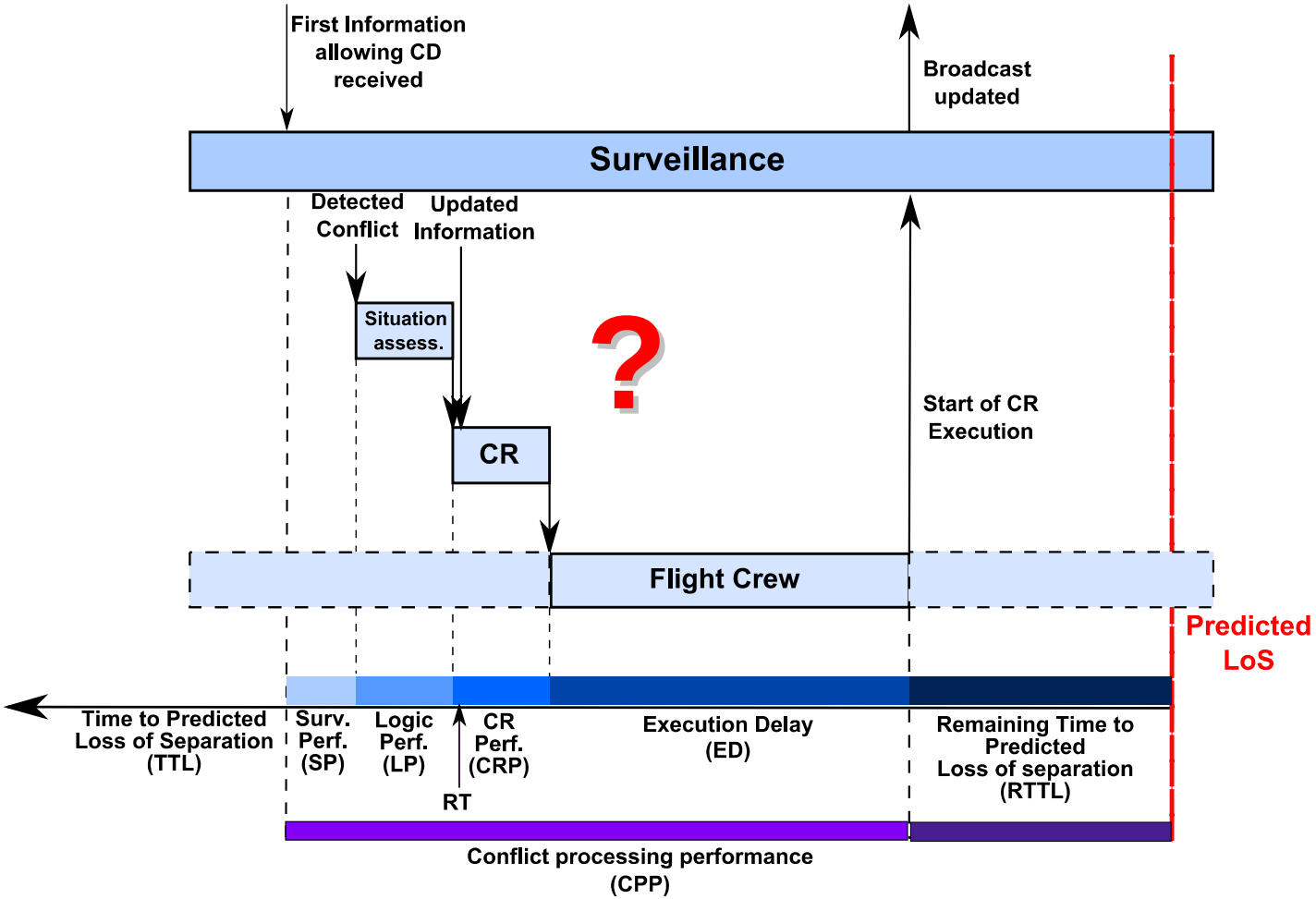
Honeywell

- Information sharing process
- Onboard conflict processing
- Communications (Data link) performance

OPA – Onboard Performance Modeling

Honeywell

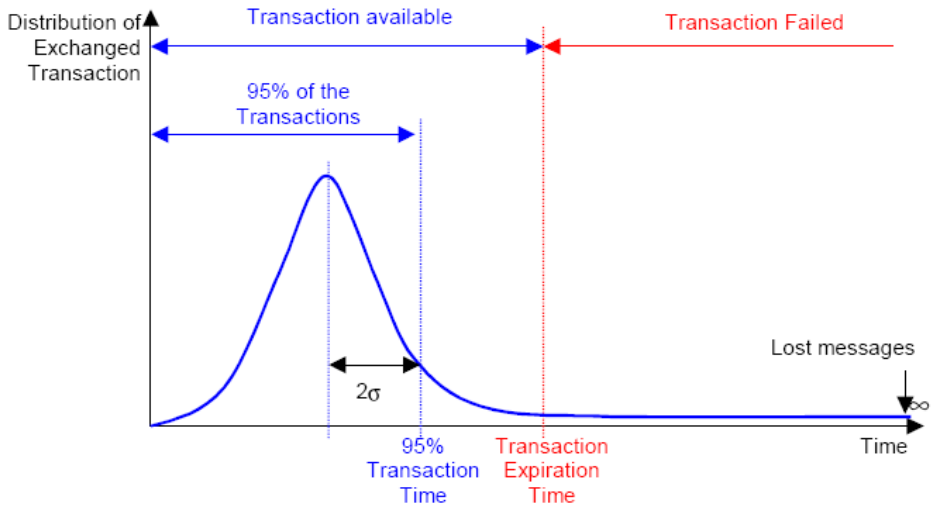
Based on the parameterization introduced by OSED (D9.1).



OPA – Communications Performance

Honeywell

- **ICAO 9869 defines Required Communication Performance (RCP) parameters**
- **OPA will perform assessment of the four RCP type parameters using the DO-264/ED-78A methodology:**
  - Maximum **transaction time** acceptable for the completion of the communication operation (normal operation is represented by a 95% transaction time);



  - **Continuity**, i.e. probability that the communication operation can be completed within the transaction time, assuming the system was available;
  - **Availability**, i.e. probability that the communication operation can be initiated when needed;
  - **Integrity**, i.e. probability the communication operation is completed with an undetected error.

Thank You!

Any Questions…

Honeywell