National Aerospace Laboratory NLR
The Netherlands

Stochastic Hybrid System Modeling, Bisimulation and Safety Verification of Airborne Self Separation

by

Henk A.P. Blom

e-mail : blom@nlr.nl

Workshop on Formal Methods in Aerospace
IEEE CDC 2010, Atlanta, GA, December 14, 2010

Key Research Question

- Free Flight (or Airborne Self Separation) has been "invented" as a potential solution for high traffic demand airspace

- ATM community research trend has been to direct Airborne Self Separation research to situations of less demanding airspace (where mid-air safety risk is coming from pairwise encounters only)

- Key research question: Up to which traffic demand can Free Flight be designed sufficiently safe ?

iFly project

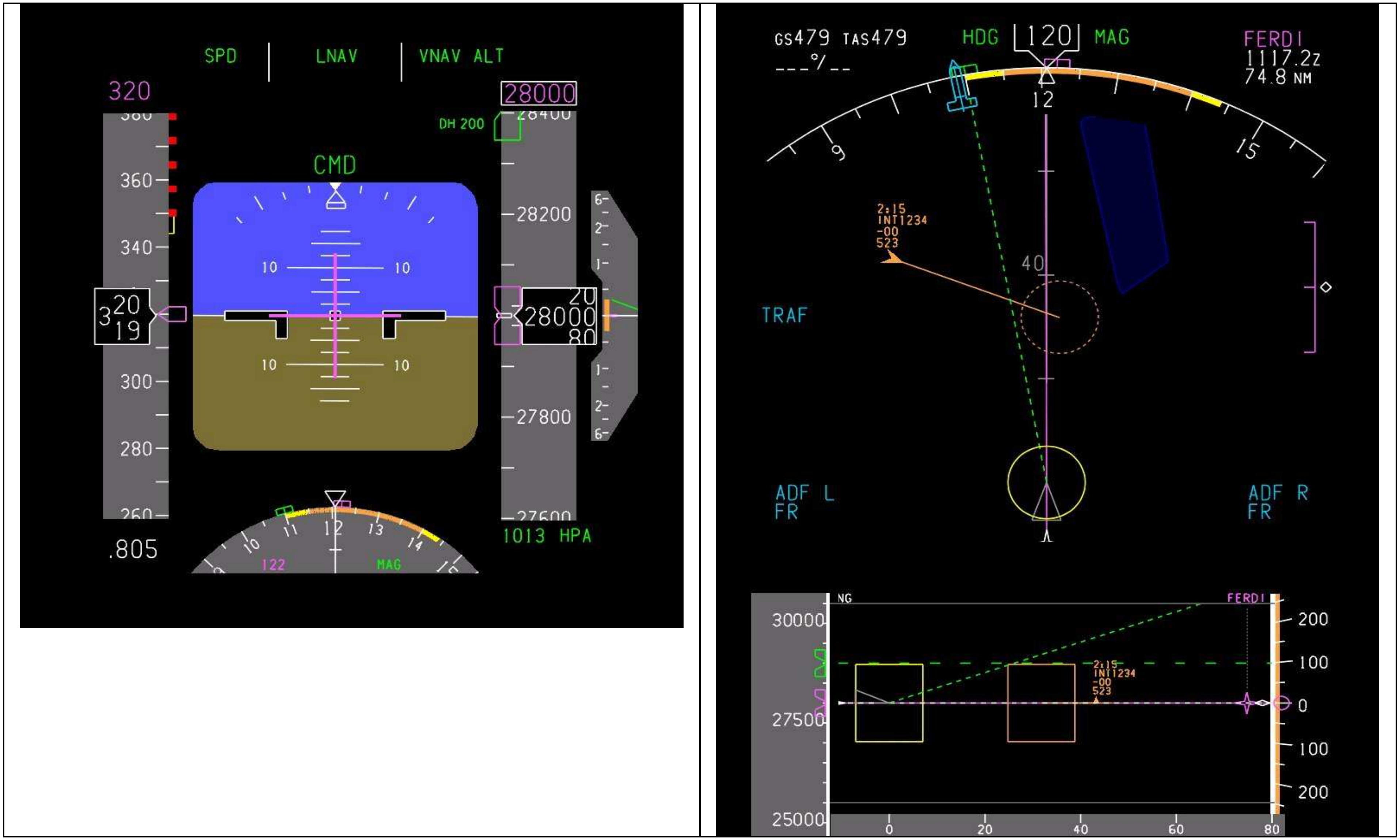
- Addresses the key research question for en-route airspace
- Approach:
  - Designing an advanced Free Flight concept of operation
  - Aiming for 3-6 times 2005 traffic demand over Europe
  - Analysing this advanced concept on mid-air safety risk
- This presentation:
  - First generation FF concept
  - Advanced FF concept
  - Safety analysis methods used
  - Results for a first generation FF concept
  - Initial results for an advanced FF concept

Stochastic Hybrid System
Modeling, Bisimulation and Safety Verification
of Airborne Self Separation

- <u>First generation Free Flight concept</u>
- Modelling and simulation
- Bisimulation
- Interacting Particle System (IPS)
- Results for 1st generation
- Advanced Free Flight concept
- Initial results for advanced FF
- Conclusions

Autonomous Mediterranean Free Flight (AMFF)

- Future concept developed for traffic over Mediterranean area
- Aircrew gets freedom to select path and speed
- In return aircrew is responsible for self-separation
- Aircraft broadcast their states without delay to other aicraft
- Each a/c equipped with an Airborne Separation Assistance System
- In AMFF, conflicts are resolved one by one (pilot preference)
  - Medium term: priority a/c does nothing
  - Short term: both aircraft resolve conflict



SPD
LNAV
VNAV ALT
320
28000
DH 200
CMD
360
340
300
280
28200
27800
1013 HPA
.805
122
MAG
GS479 TAS479
HDG
120
MAG
FERDI
1117.2z
74.8 NM
2:15
INT1234
-00
523
TRAF
40
ADF L
FR
ADF R
FR
NG
FERDI
30000
27500
25000
200
100
0
100
200
0
20
40
60
80

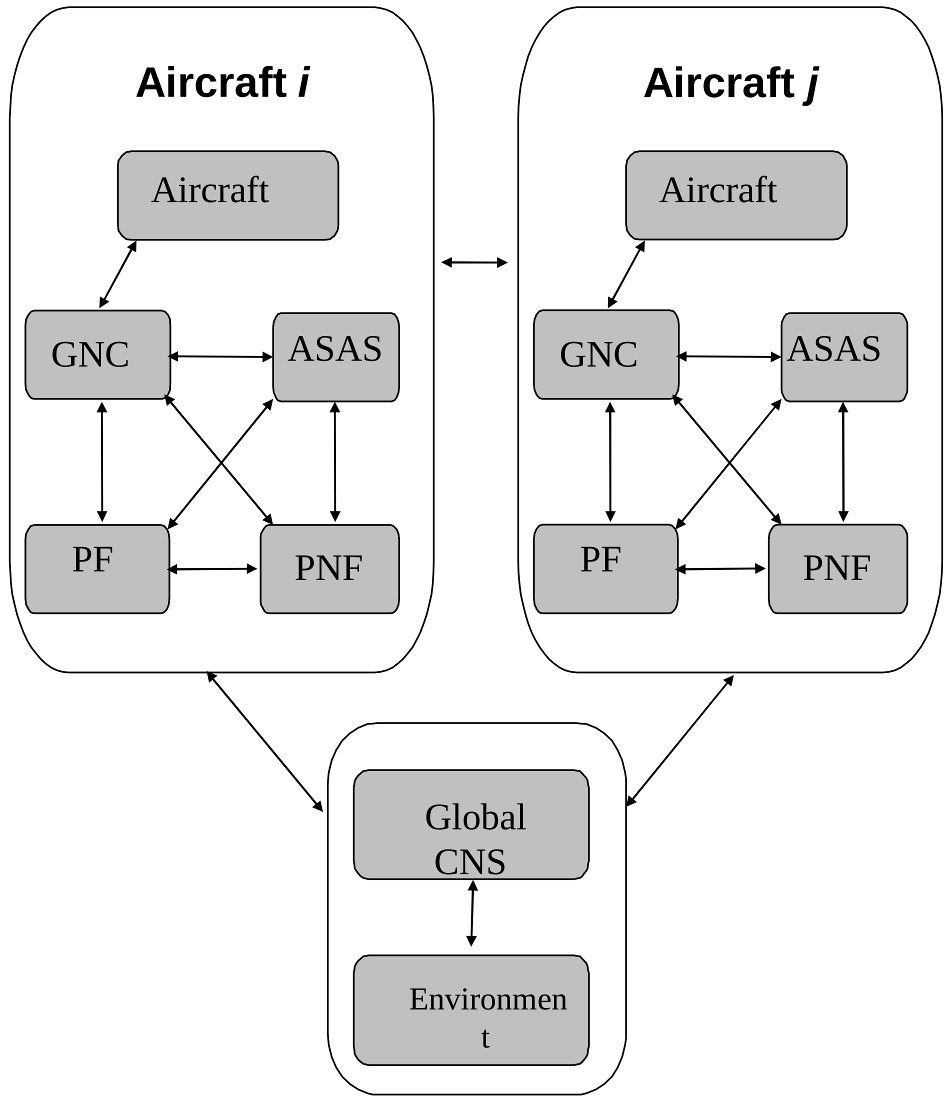
Evaluations performed for AMFF concept

- Real-time pilot-in-the-loop evaluations
- Eurocae/RTCA ED78a safety assessment

Stochastic Hybrid System Modeling, Bisimulation and Safety Verification of Airborne Self Separation

- First generation Free Flight concept
- <u>Modelling and simulation</u>
- Bisimulation
- Interacting Particle System (IPS)
- Results for 1st generation
- Advanced Free Flight concept
- Initial results for advanced FF
- Conclusions

Multiple Agents in Airborne Self Separation

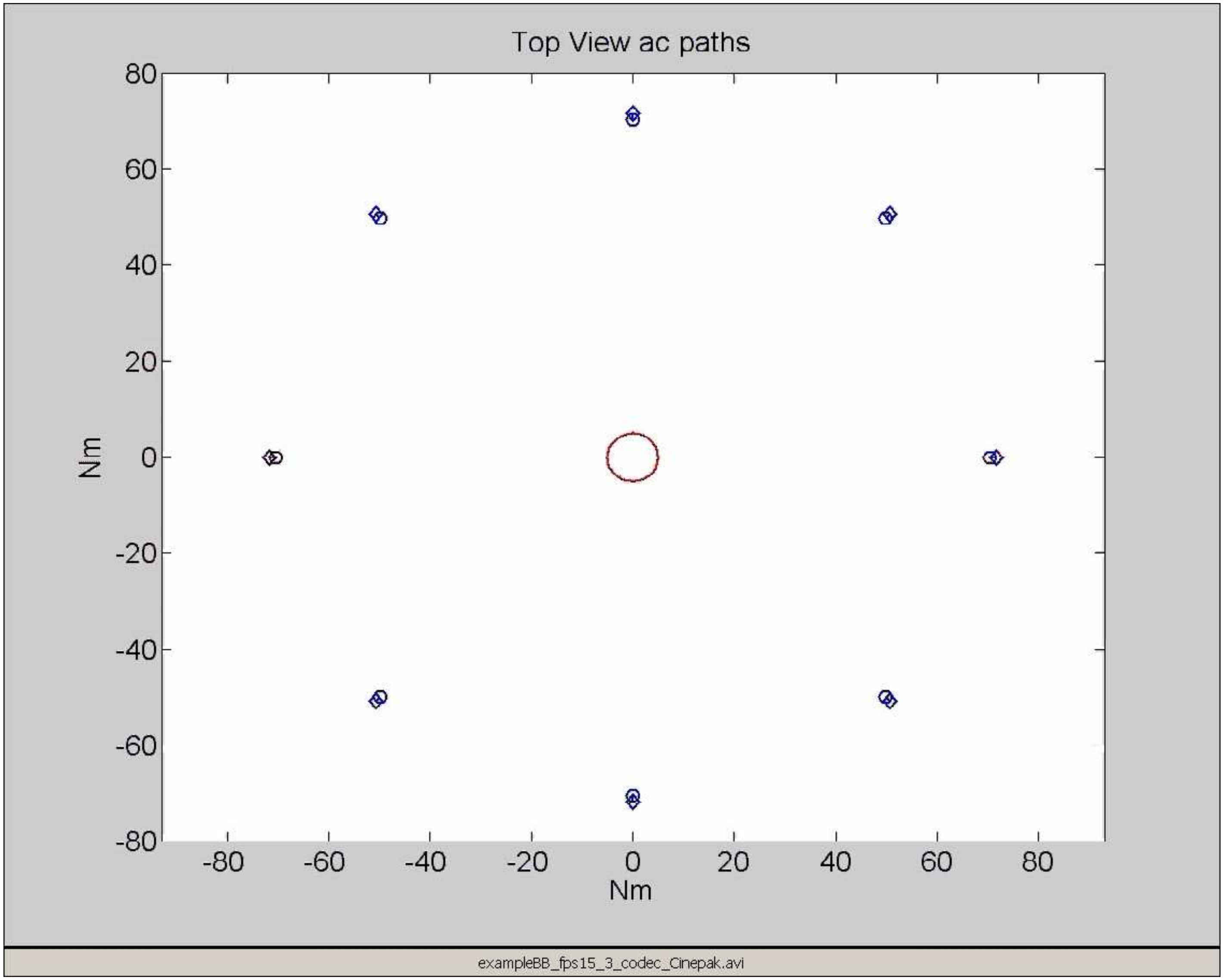


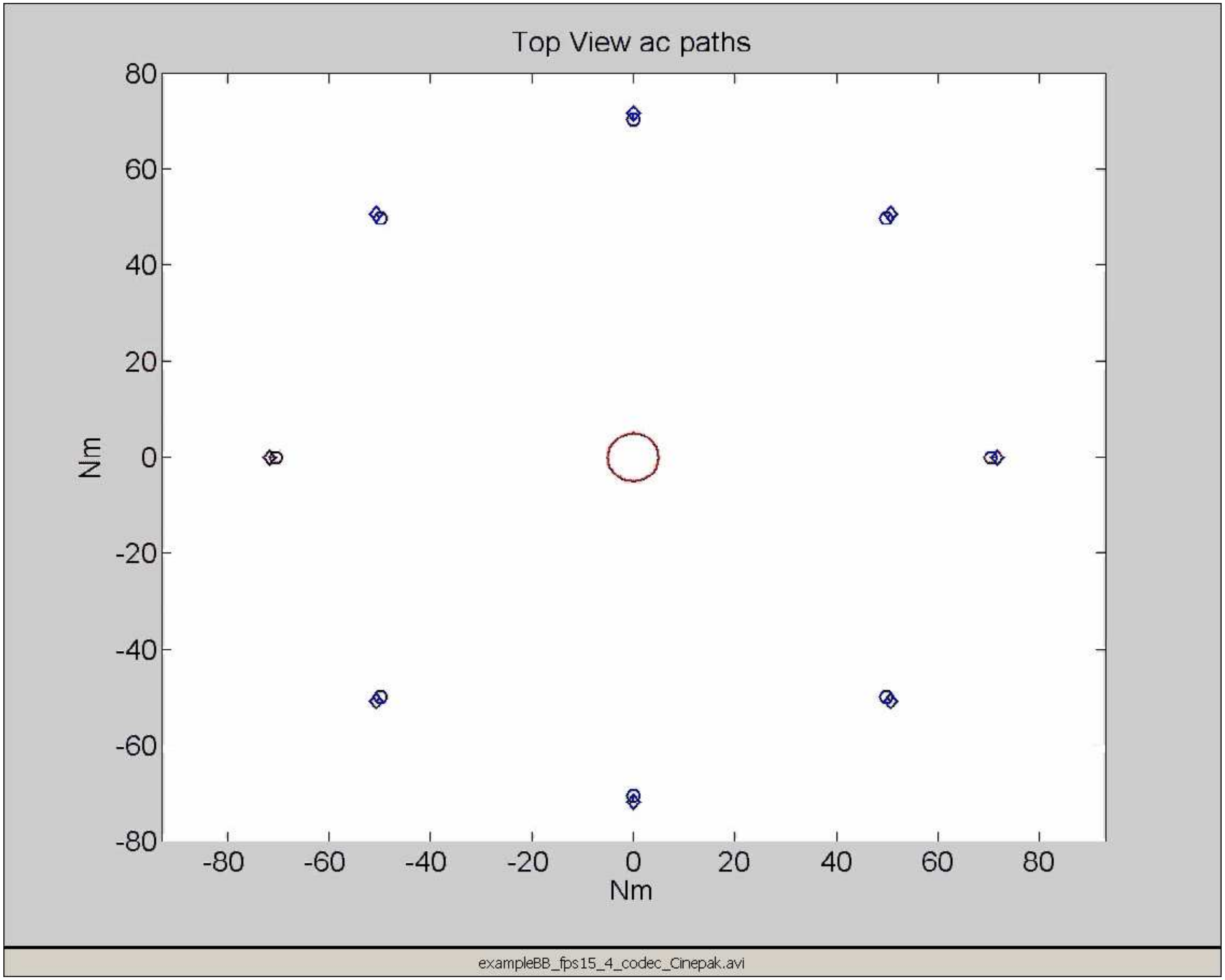
Development of SDCPN model

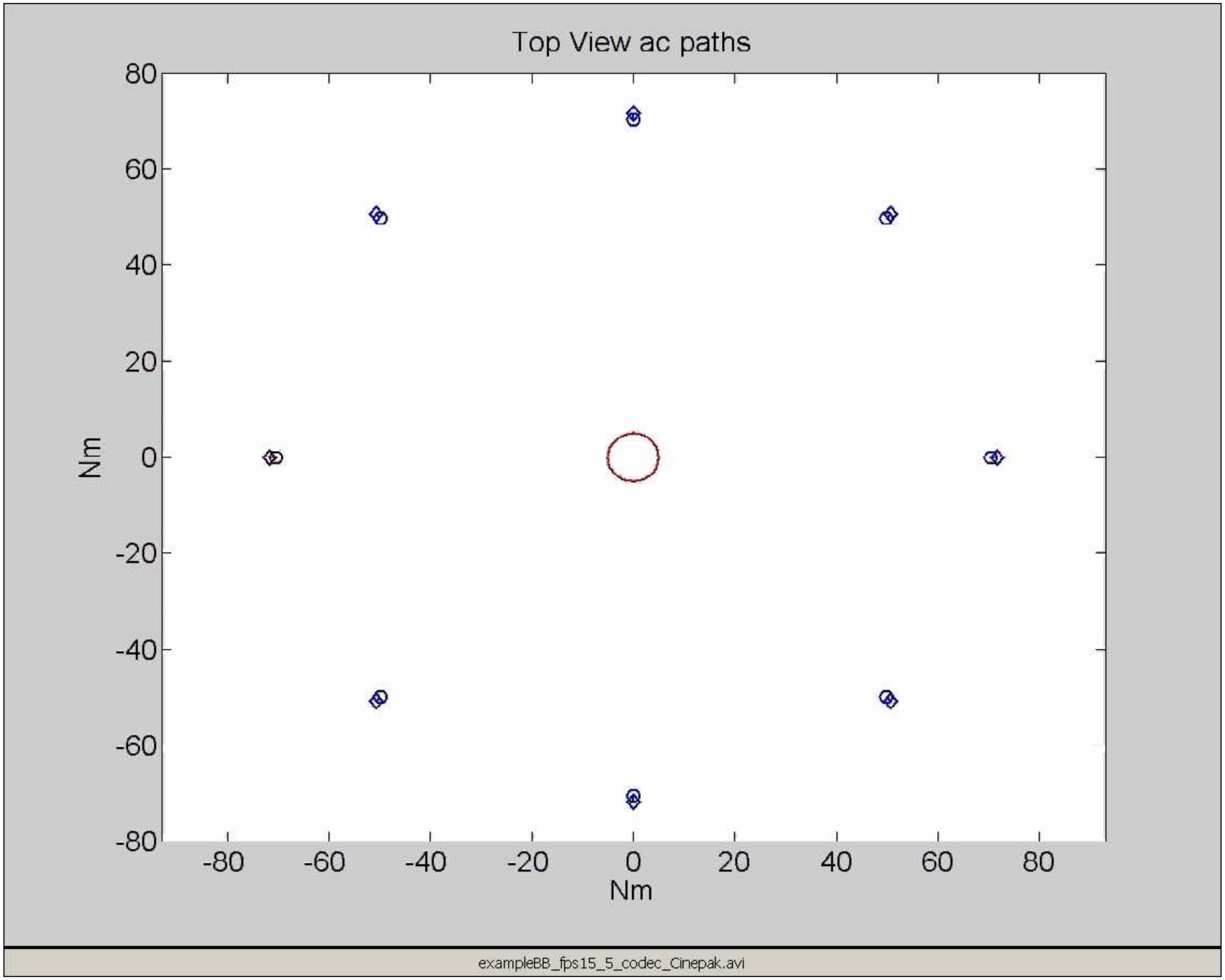
- Defining the relevant Agents
- Hazard identification
- Developing Petri net for each Agent
- Connecting Agent Petri nets
- Generate Monte Carlo simulation model
- Parametrization, Verification & Calibration

Size of an airborne self separation model

Agent	# of product places	Maximum colour Product state space
Aircraft	24^N	R^{13N}
Pilot-Flying (PF)	490^N	R^{28N}
Pilot-not-Flying (PNF)	7^N	R^{3N}
AGNC	$(15\times 2^{16})^N$	R^{45N}
ASAS	48^N	$R^{37N+21N^2}$
Global CNS	16	R^0
PRODUCT	$\approx 16\times(3.88\times 10^{12})^N$	$R^{126N+21N^2}$


Top View ac paths
80
60
40
20
0
-20
-40
-60
-80
Nm
-80
-60
-40
-20
0
20
40
60
80
Nm
exampleBB_fps15_3_codec_Cinepak.avi


Top View ac paths
80
60
40
20
0
-20
-40
-60
-80
Nm
-80 -60 -40 -20 0 20 40 60 80
Nm
exampleBB_fps15_4_codec_Cinepak.avi

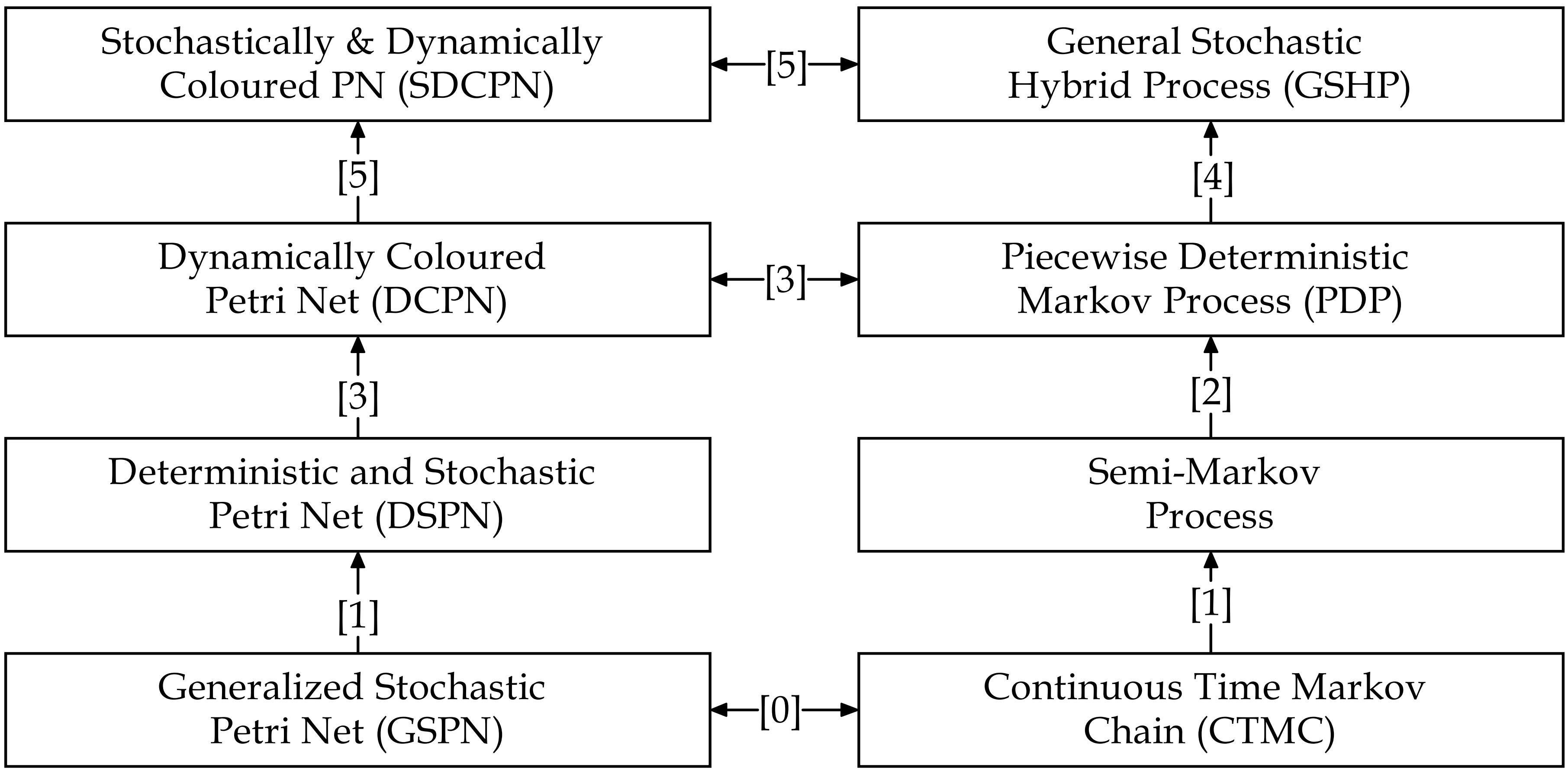


Top View ac paths
80
60
40
20
0
-20
-40
-60
-80
Nm
-80 -60 -40 -20 0 20 40 60 80
Nm
exampleBB_fps15_5_codec_Cinepak.avi

Stochastic Hybrid System Modeling, Bisimulation and Safety Verification of Airborne Self Separation

- First generation Free Flight concept
- Modelling and simulation
- <u>Bisimulation</u>
- Interacting Particle System (IPS)
- Results for 1st generation
- Advanced Free Flight concept
- Initial results for advanced FF
- Conclusions

Modelling Power Hierarchy



[0]: [Ajmone Marsan, 1990]

[1]: [Malhotra & Trivedi, 2004], [Muppala et al, 2000]

[2]: [Davis, 1984]

[3]: [Everdij & Blom, 2005]

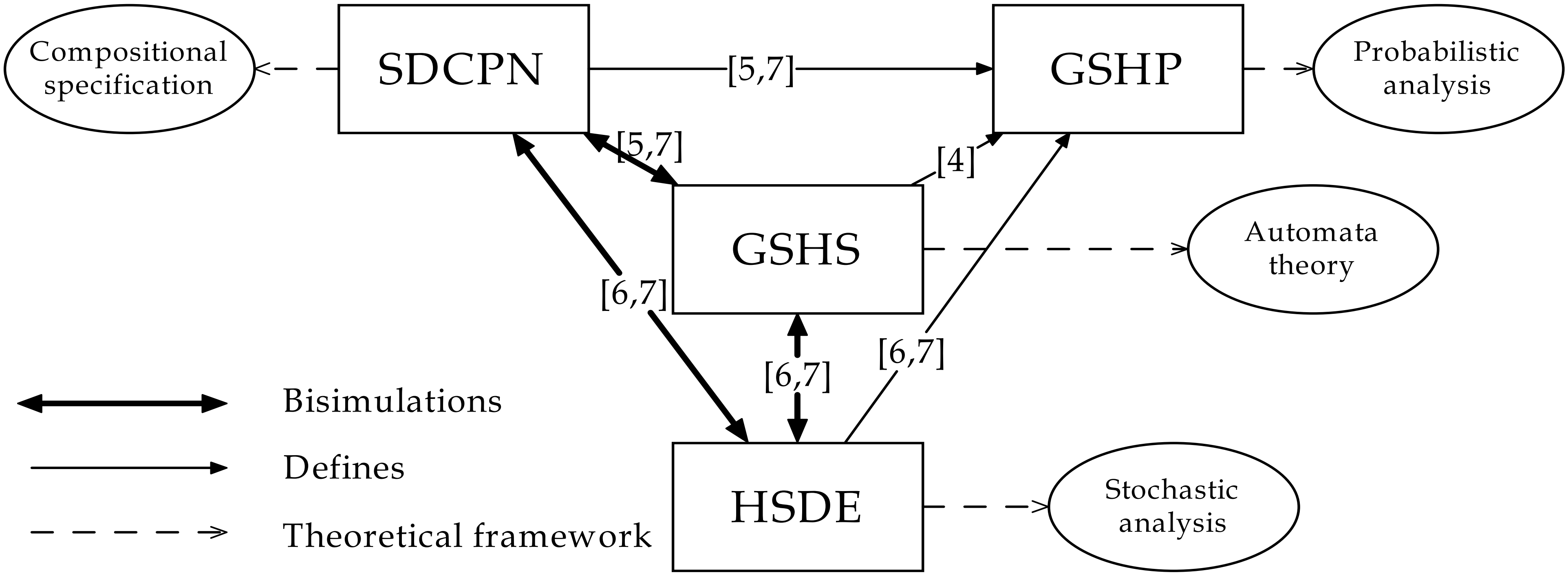
[4]: [Bujorianu & Lygeros, 2006]

[5]: [Everdij & Blom, 2006]

Bisimulation

- Two systems are bisimulations when their executions are equivalent in probabilistic sense
  - VanDerSchaft, 2004; Bujorianu et al., 2005
- Systems with GSHP executions:
  - SDCPN = Stochastically and Dynamically Coloured Petri Net
  - GSHS = General Stochastic Hybrid System
  - HSDE = Hybrid Stochastic Differential Equation

SDCPN inherits analysis power of SDE's and formal verification power of automata



[4]: [Bujorianu & Lygeros, 2006]

[5]: [Everdij & Blom, 2006]

[6]: [Everdij & Blom, 2010]

[7]: [Everdij, 2010]

Stochastic Hybrid System
Modeling, Bisimulation and Safety Verification
of Airborne Self Separation

- First generation Free Flight concept
- Modelling and simulation
- Bisimulation
- <u>Interacting Particle System (IPS)</u>
- Results for 1st generation
- Advanced Free Flight concept
- Initial results for advanced FF
- Conclusions

Approaches in Reach Probability Computation

- Markov Chain (MC) approximation (Prandini&Hu, 2006)
- Dynamic Programming (DP) approach (Abate, Amin, Prandini, Lygeros & Sastry, 2006)
- Interacting Particle System (IPS) approach (Cerou et al., 2005)

Interacting Particle System (IPS)

- Define a sequence of conflict levels decreasing in urgency $(D_k\text{'s})$
  - Most urgent level represents collision $(D_m = D)$
- Simulate N_p particles; initially all outside D_1 (less urgent level)
- Freeze each particle that reaches the next urgent level before T
- Make N_p copies of frozen particles
- Repeat this until the most urgent level has been reached
- Count the simulated fraction $\tilde{\gamma}_k$ that reaches level k
- Estimated collision risk = $\tilde{\gamma}_1 \times \tilde{\gamma}_2 \times \tilde{\gamma}_3 \times \ldots \times \tilde{\gamma}_m$

IPS convergence

Cerou, Del Moral, Legland and Lezaud (2002, 2005) have shown that the product of these fractions $\tilde{\gamma}_k$ forms an unbiased estimate of the probability of $\{s_t\}$ to hit the set D within the time period $[0,T)$, i.e.

$$\mathbb{E}[\prod_{k=1}^{m} \tilde{\gamma}_k] = \prod_{k=1}^{m} \gamma_k = P(\tau < T)$$

In addition there is a bound on the L^1 estimation error, i.e.:

$$\mathbb{E}(\prod_{k=1}^{m} \tilde{\gamma}_k - \prod_{k=1}^{m} \gamma_k) \leq \frac{c_p}{\sqrt{N_p}}$$

Hybrid IPS versions

1. Importance switching (Krystul&Blom, 2005)

2. Rao-Blackwellization, using exact equations for $\{\theta_t\}$ and particles for Euclidian state (Krystul&Blom, 2006)

- Both handle rare mode switching well
- Large scale SHS scalability problem remains
  - Huge number of discrete product places

Hierarchical Hybrid IPS (HHIPS)

(Blom, Bakker & Krystul, 2007, 2009)

- ✓ Define an aggregated mode process $\{\kappa_t\}$ with $\{\mathbb{M}_k,\ \kappa \in \mathbb{K}\}$ a partition of $\mathbb{M}$

$$\kappa_t = \kappa \ \text{ if } \theta_t \in \mathbb{M}_k$$

- ✓ Apply Importance switching to $\{\kappa_t\}$
- ✓ Rao-Blackwellization, i.e. use exact equations for $\{\kappa_t\}$ and particles for the other process elements $\{x_t, \theta_t\}$

Stochastic Hybrid System Modeling, Bisimulation and Safety Verification of Airborne Self Separation

- First generation Free Flight concept
- Modelling and simulation
- Bisimulation
- Interacting Particle System (IPS)
- <u>Results for 1st Generation</u>
- Advanced Free Flight concept
- Initial results for advanced FF
- Conclusions

Scenarios

- Two aircraft encounter
- Eight aircraft encounter
- Random traffic

Sequence of conflict levels for air traffic

k	1	2	3	4	5	6	7	8
D_k (Nm)	4.5	4.5	4.5	4.5	2.5	1.25	0.5	0.054
h_k (ft)	900	900	900	900	900	500	250	131
Δ_k (min)	8	2.5	1.5	0	0	0	0	0

Medium Term Conflict (MTC)

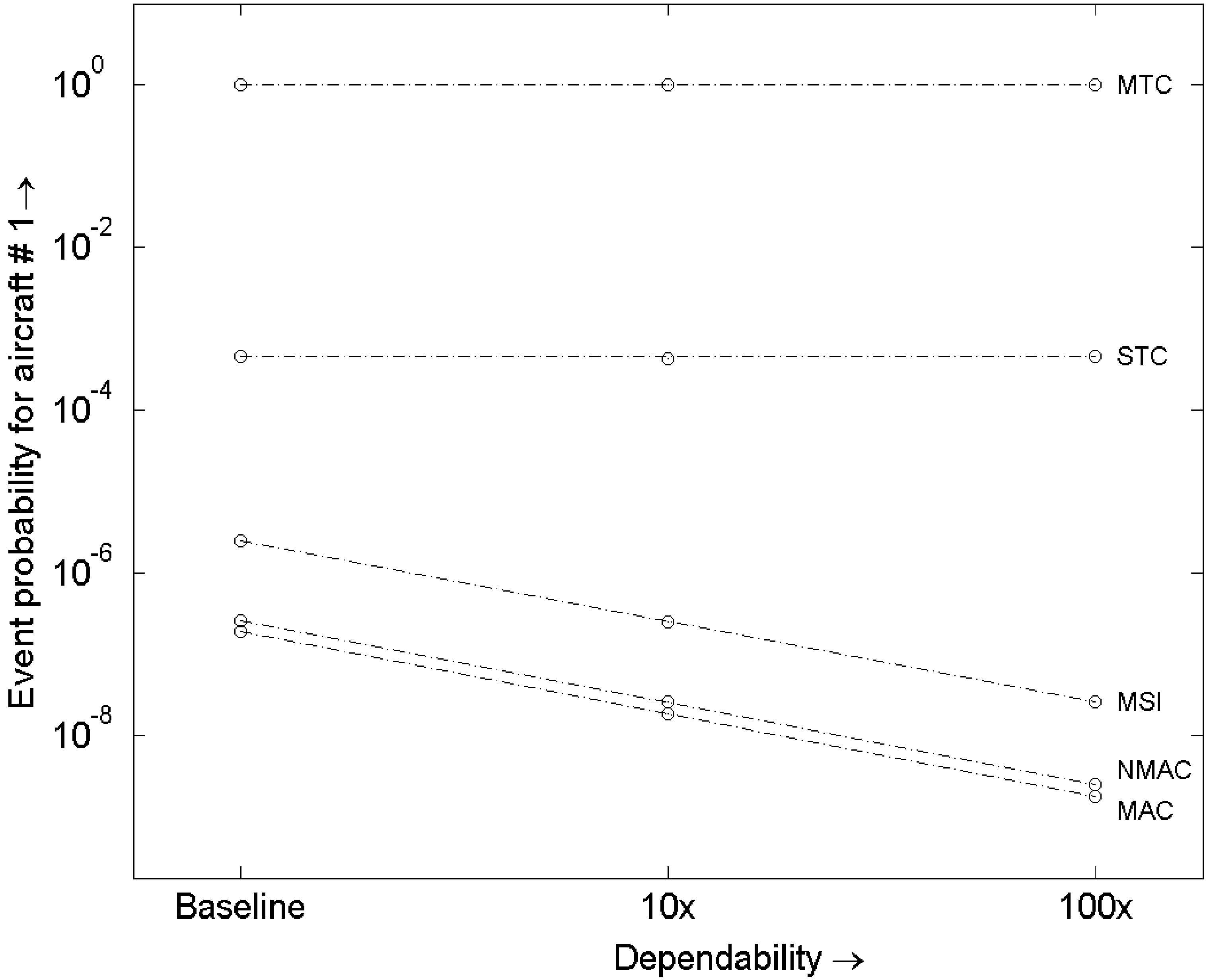
Short Term Conflict (STC)

Minimum Separation Infringement (MSI)

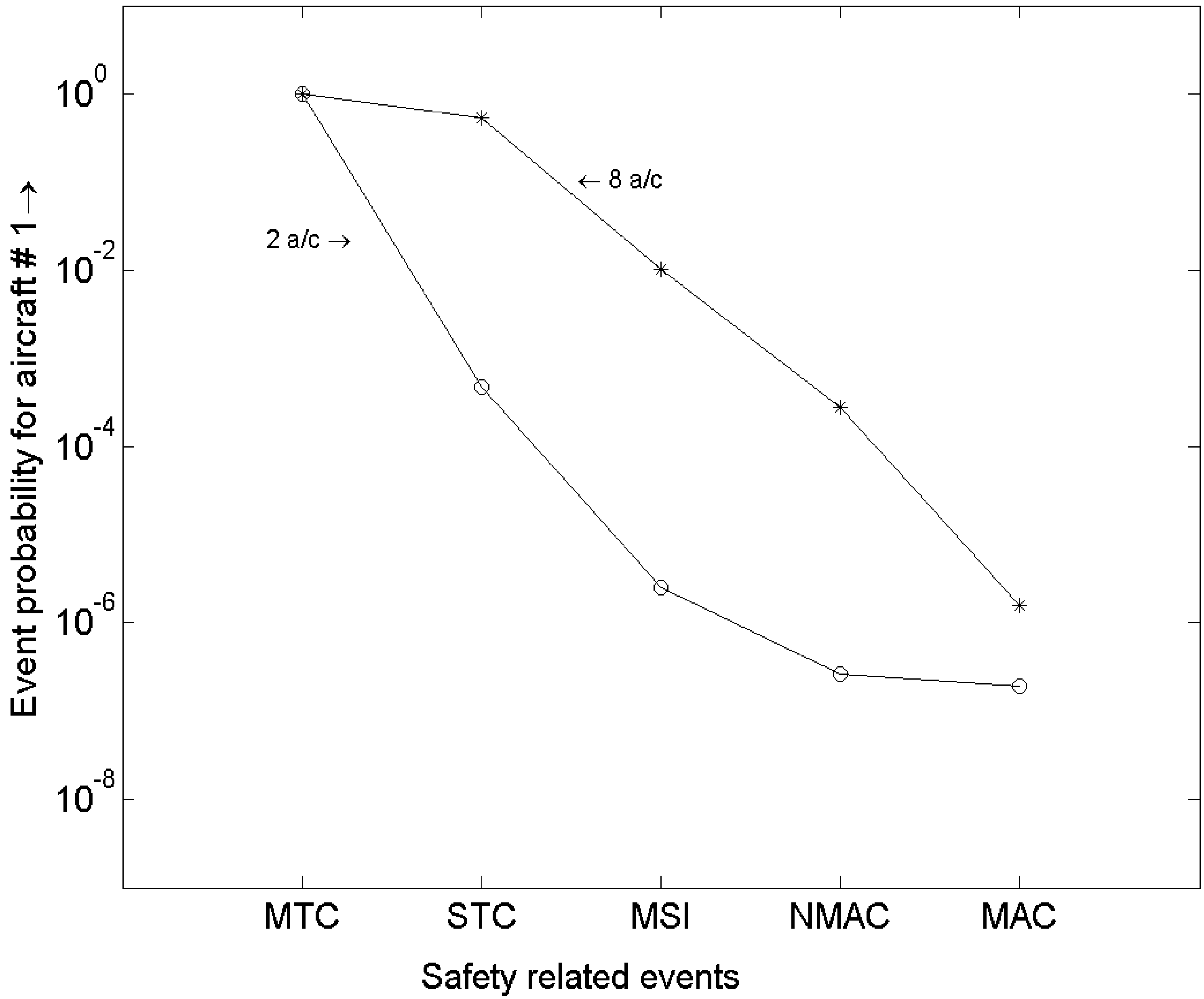
Near Mid-Air Collision (NMAC)

Mid-Air Collision (MAC)

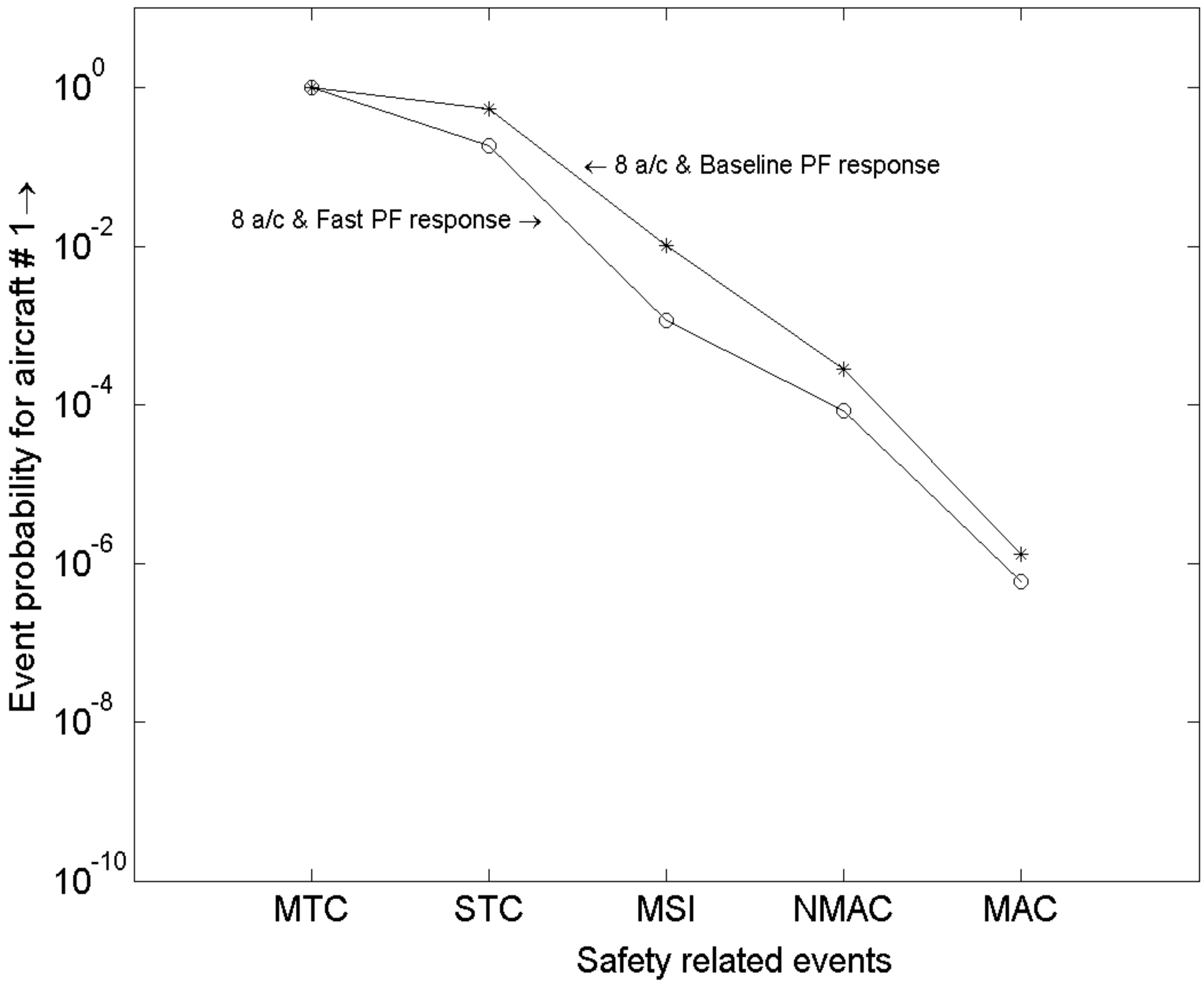
Two-aircraft encounter and dependable technical systems



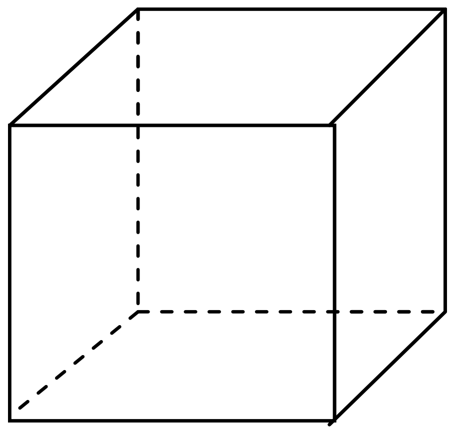
Two-aircraft vs. eight-aircraft encounter



Eight-aircraft encounter: Baseline PF response vs. Fast PF response

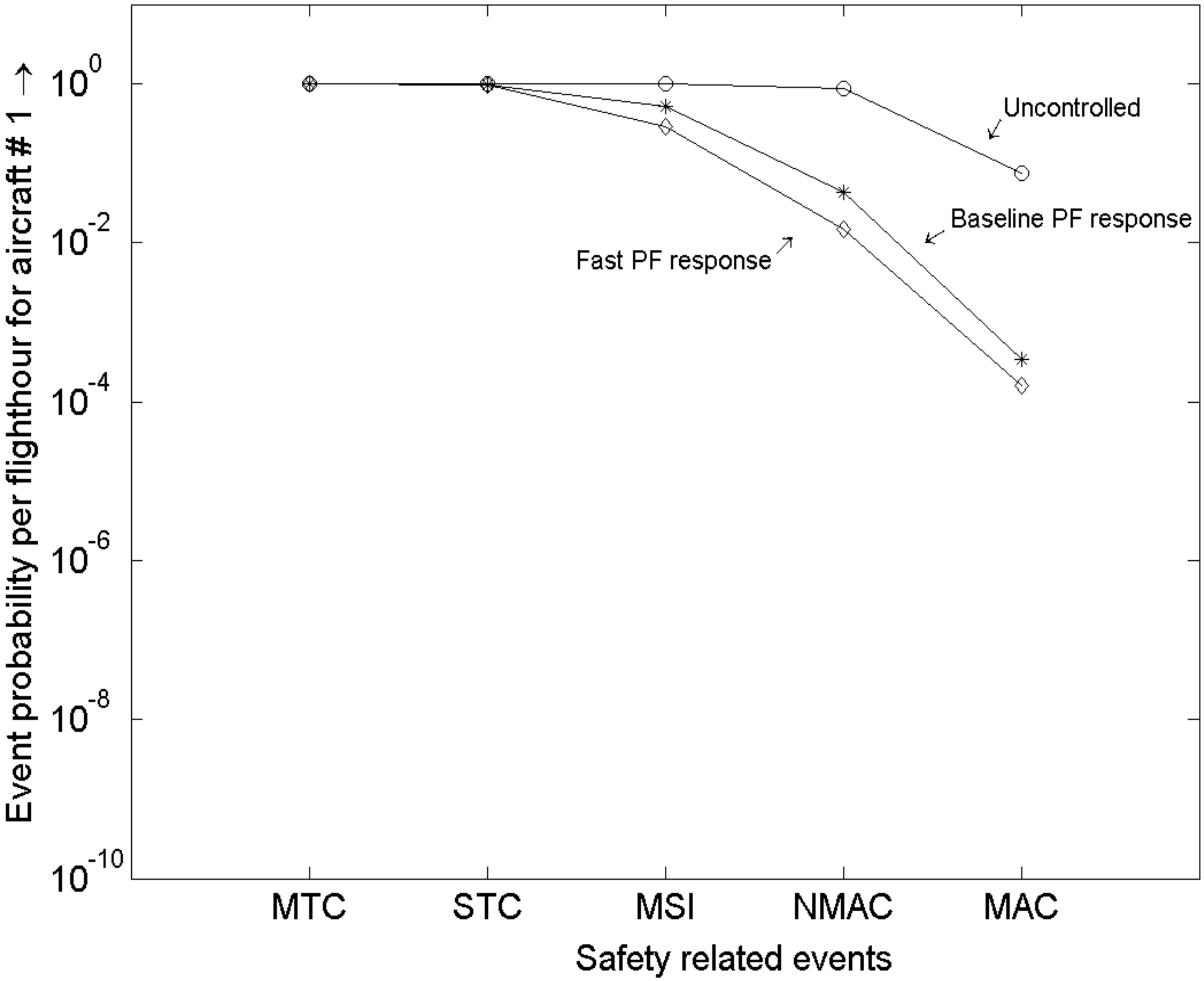


Random traffic, high density



- **Eight aircraft per packed container**
  - 3 times as dense above Frankfurt on 23rd July ’99

Random high traffic: Uncontrolled vs. AMFF controlled



Stochastic Hybrid System Modeling, Bisimulation and Safety Verification of Airborne Self Separation

- First generation Free Flight concept
- Modelling and simulation
- Bisimulation
- Interacting Particle System (IPS)
- Results for 1st generation
- Advanced Free Flight concept
- Initial results for advanced FF
- Conclusions

iFly developed advanced FF concept

- Future concept developed for high demand En Route areas

- Inputs used:
  - Advanced FF concept developed by NASA
  - Learning from AMFF safety analysis

- Communication means:
  - ADS-B between aircraft within line of sight
  - SWIM between aircraft over the horizon

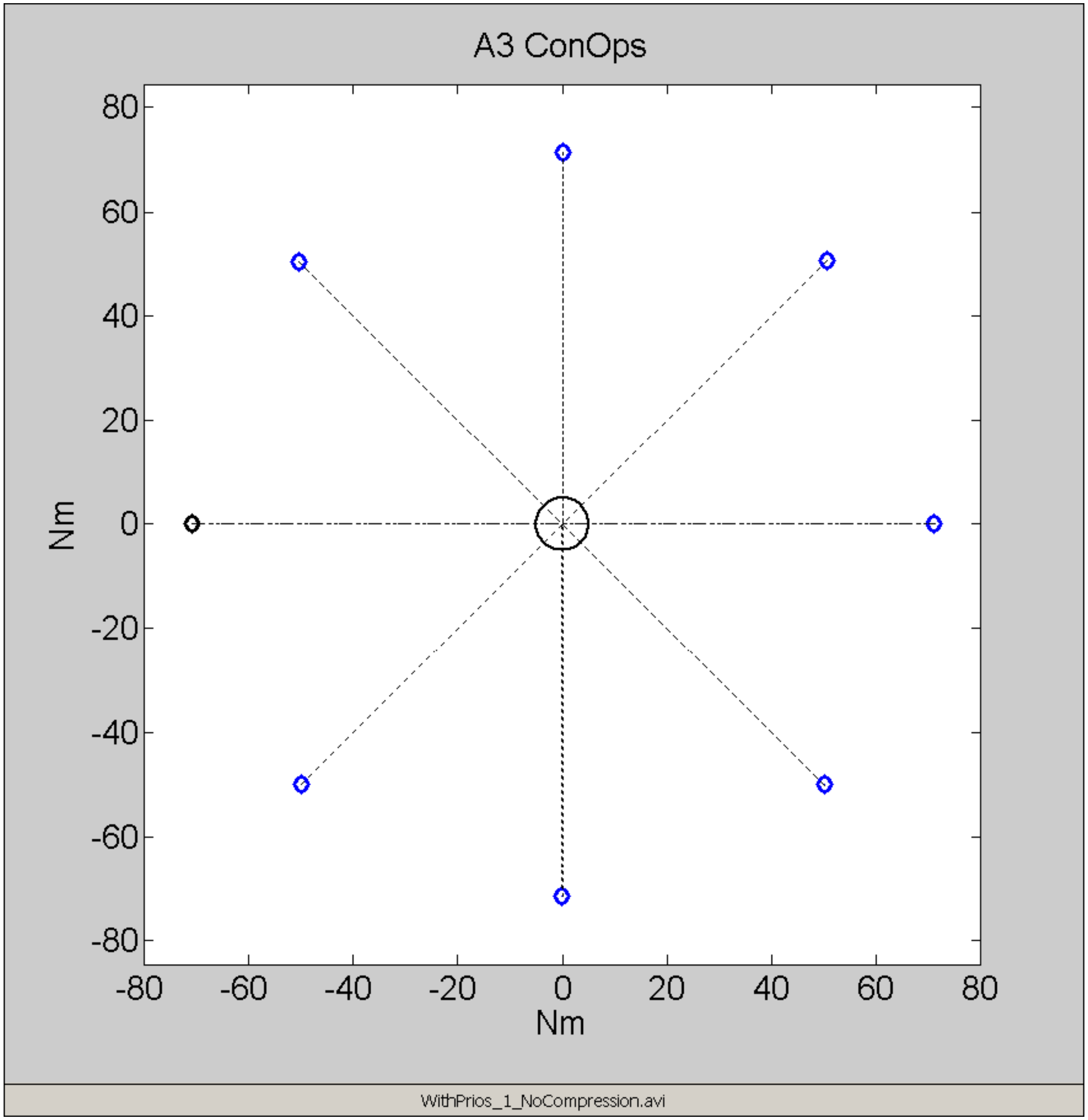
- Each aircraft receives
  - State updates by other aircraft without delay
  - Intent updates by other aircraft with some delay

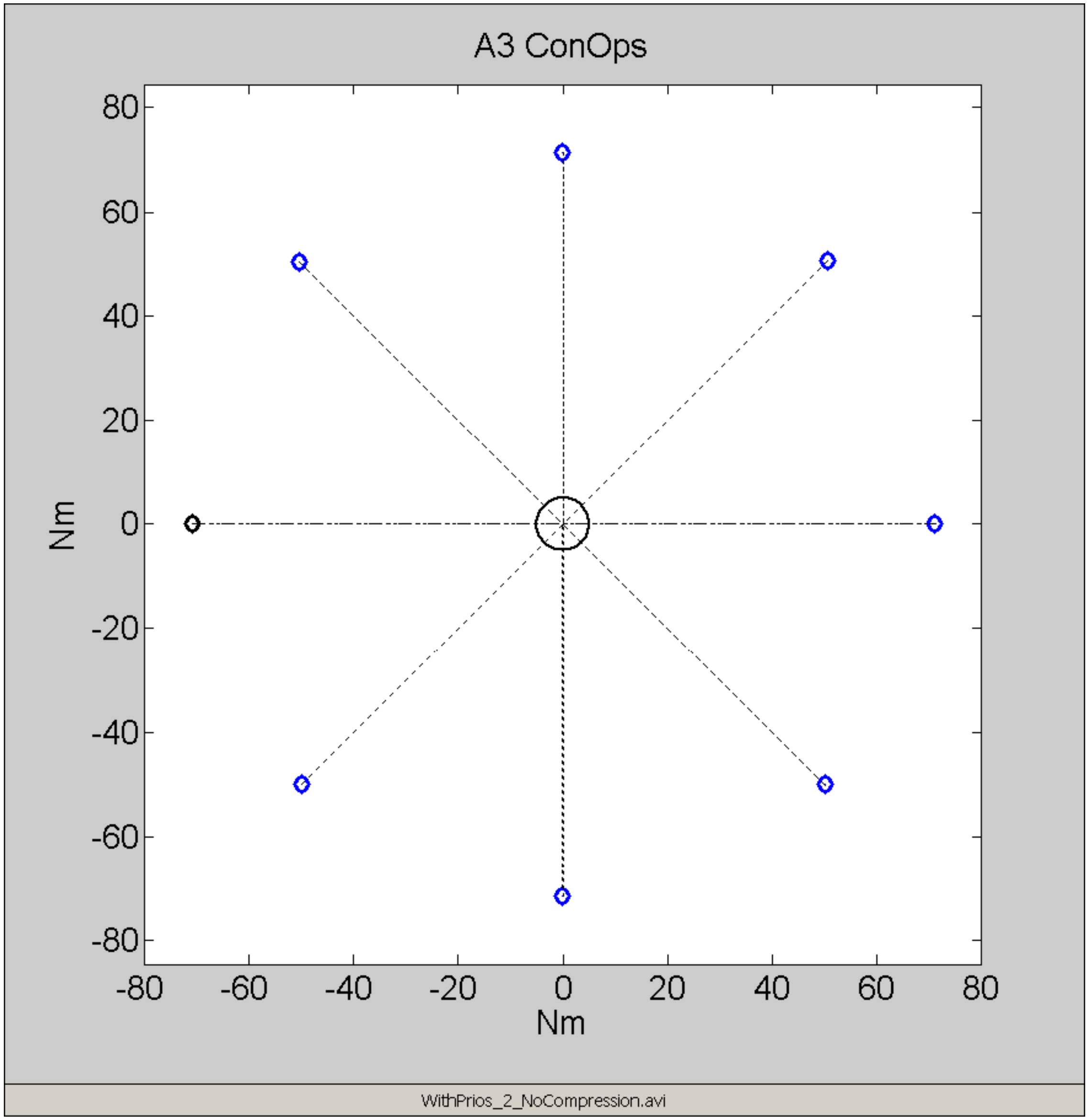
- Each a/c equipped with an advanced ASAS, which resolves:
  - Medium term conflicts: a higher priority a/c does not need to resolve
  - Short term conflicts: all aircraft involved help resolving

Candidate resolution algorithms

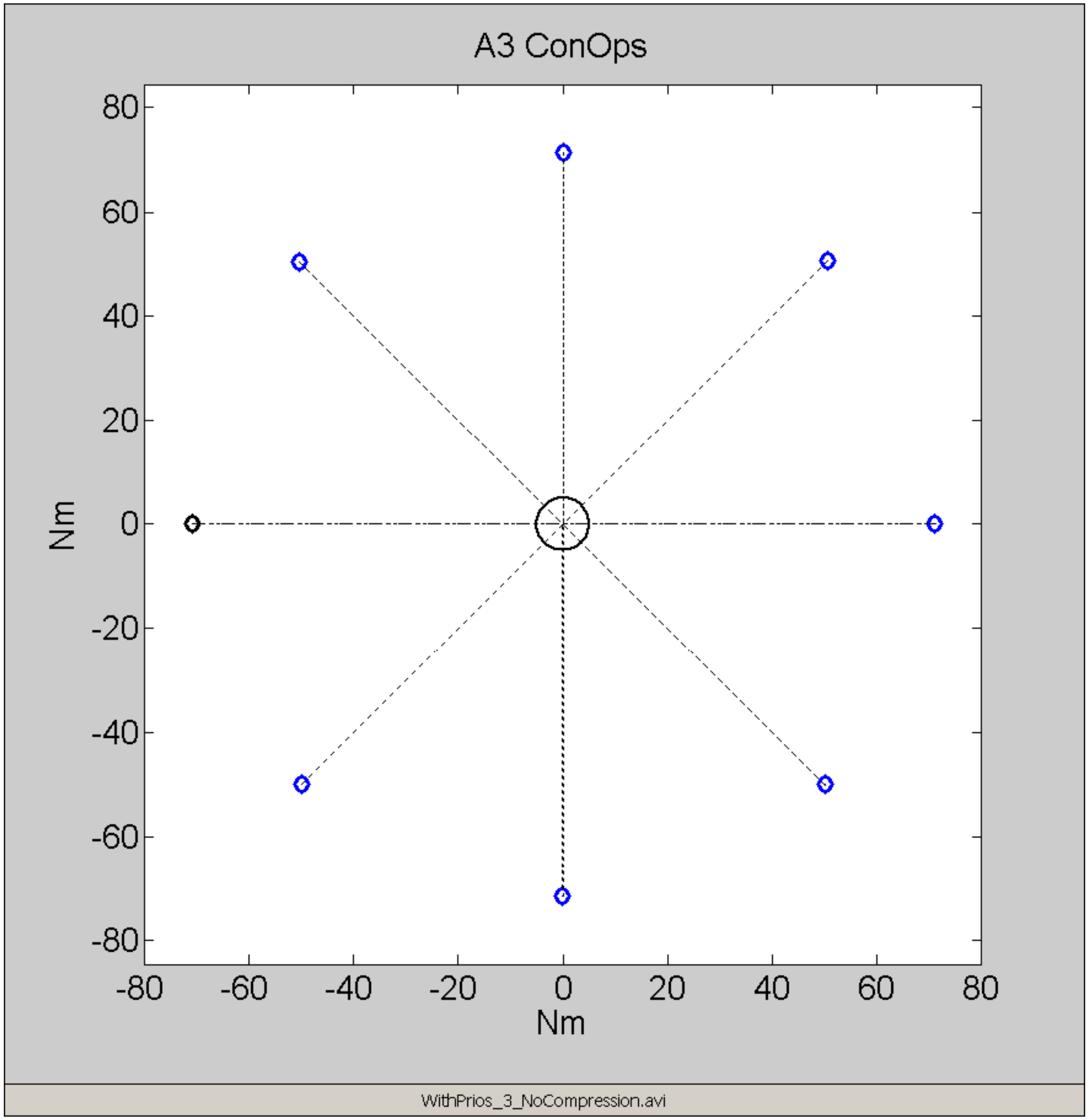
- Short Term conflict resolution (3 minutes horizon):
  - Navigation Functions based escapes
  - Velocity Obstacles (VO) based escapes

- Medium Term conflict resolution (6 minutes horizon):
  - Genetic Algorithm based intents
  - Multiplexed Model Predictive Control based intents
  - Combinatorial Optimization based intents
  - Velocity Obstacles (VO) based intents

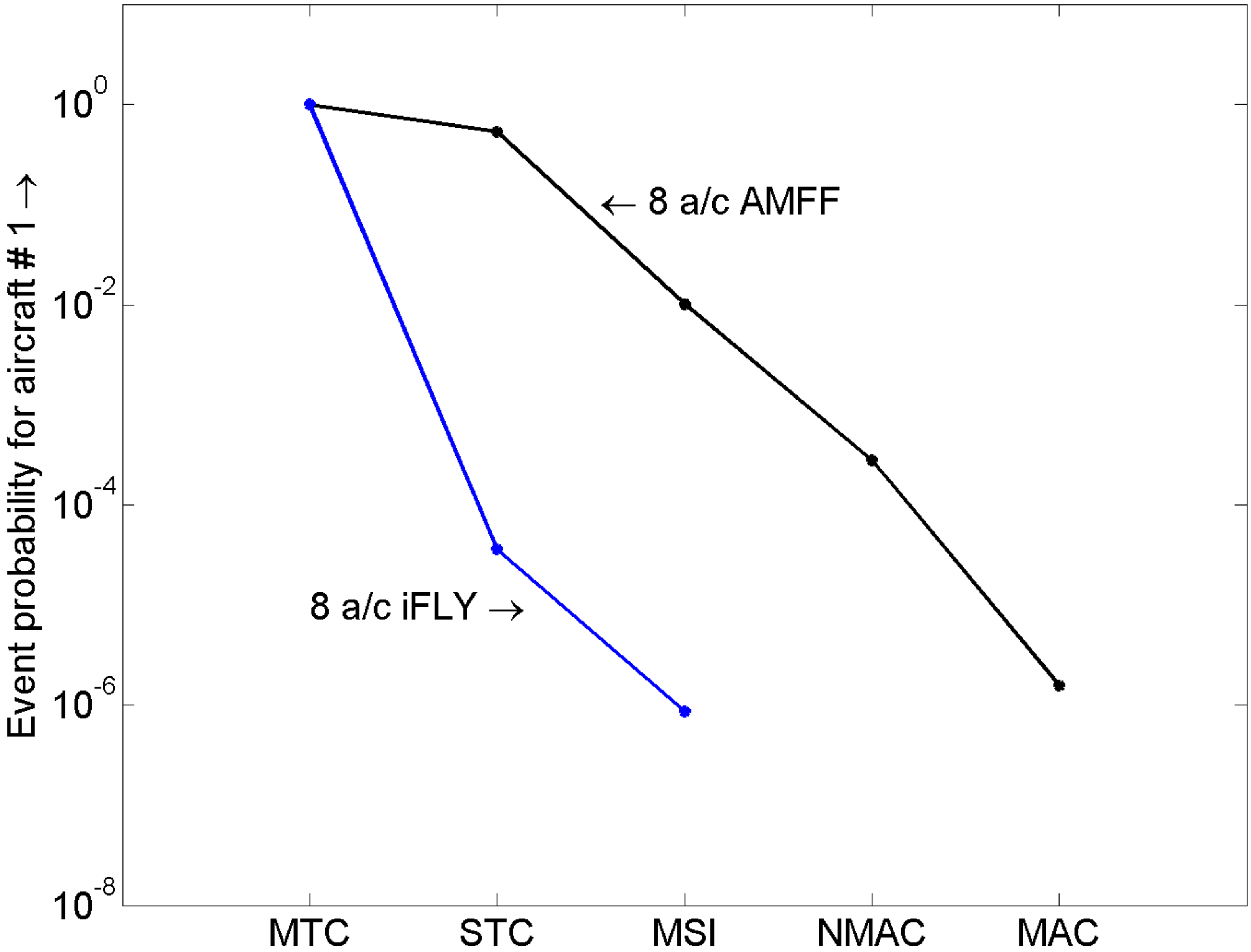

A3 ConOps
80
60
40
20
0
-20
-40
-60
-80
Nm
-80
-60
-40
-20
0
20
40
60
80
Nm
WithPrios_1_NoCompression.avi



A3 ConOps
80
60
40
20
0
-20
-40
-60
-80
Nm
-80 -60 -40 -20 0 20 40 60 80
Nm
WithPrios_2_NoCompression.avi


A3 ConOps
80
60
40
20
0
-20
-40
-60
-80
Nm
-80 -60 -40 -20 0 20 40 60 80
Nm
WithPrios_3_NoCompression.avi

Eight-aircraft encounter; iFLY vs. AMFF



Stochastic Hybrid System Modeling, Bisimulation and Safety Verification of Airborne Self Separation

- First generation Free Flight concept
- Modelling and simulation
- Bisimulation
- Interacting Particle System (IPS)
- Results for 1st generation
- Advanced Free Flight concept
- Initial results for advanced FF
- Conclusions

Conclusions

- Outstanding Key research question: Up to which traffic demand can be safely accommodated by Free Flight (or Airborne Self Separation) ?

- This presentation has given an overview of safety verification approach:
  - SHS modelling framework
  - Bisimilarity relations
  - Monte Carlo speed-up

- Application to AMFF and advanced FF showed:
  - 1st Generation FF cannot accomodate high traffic demands
  - Advanced FF characteristics look very promising

Follow-up

- Follow-up work on advanced FF concept:
  - Continue resolution algorithm developments
  - Emphasis on efficiency of resolutions
  - Lygeros, Maciejowski, Kyriakopoulos and co-workers

- Follow-up work on risk assessment:
  - Continue evaluation of advanced FF concept using VO
  - Further enhancement of HHIPS
  - Include ACAS in simulation model
  - Validation of assessed risk level

- http://iFly.nlr.nl

Validation of assessed risk level

- **Simulation model ≠ Reality**
- Identify the differences
- Assess each difference individually (and conditionally)
  - use of statistical data and expert knowledge
- Assess model parameter sensitivities by Monte Carlo simulations
- Evaluate effect of each assumption at simulated risk level
  - use of statistical data and expert knowledge
- Evaluate combined effects of all model assumptions
  - Typical output: expected risk and 95% area
- Improve simulation model for large differences

Questions / Discussion

References (1/3)

[Ajmone Marsan, 1990] M. Ajmone Marsan, Stochastic Petri nets: an elementary introduction, In: G. Rozenberg, Advances in Petri nets 1989, Lecture notes in Computer Science Vol. 424, Springer, 1990, pp. 1-29.

[Muppala et al, 2000] J.K. Muppala, R.M. Fricks, K.S. Trivedi, Techniques for system dependability evaluation, In: W. Grasman, Computational probability, Kluwer, 2000, pp. 445-480.

[Malhotra&Trivedi, 2004] M. Malhotra, K.S. Trivedi, Power hierarchy of dependability model types, IEEE Tr. Reliability, Vol. 43 (1994), pp. 493-502.

[Davis, 1984] M.H.A. Davis, Piecewise Deterministic Markov processes: a general class of non-diffusion stochastic models, Journal Royal Statistical Society (B), Vol. 46, 1984, pp. 353-388.

[Everdij&Blom, 2005] M.H.C. Everdij, H.A.P. Blom, Piecewise Deterministic Markov processes represented by dynamically coloured Petri nets, Stochastics, Vol. 77 (2005), pp. 1-29.

[Bujorianu&Lygeros, 2006] M.L. Bujorianu and J. Lygeros. Toward a general theory of stochastic hybrid systems. In: H.A.P. Blom and J. Lygeros, *Stochastic hybrid systems: theory and safety critical applications*, volume 337 of *Lectures notes in control and information sciences (LNCIS)*, Vol. 337, Springer, 2006, pp. 3-30.

[Everdij&Blom, 2006] M.H.C. Everdij and H.A.P. Blom. Hybrid Petri nets with diffusion that have into-mappings with generalised stochastic hybrid processes. In: H.A.P. Blom and J. Lygeros, *Stochastic hybrid systems: theory and safety critical applications*, *Lectures notes in control and information sciences (LNCIS)* Vol. 337, Springer, 2006, pp. 31–63.

- References (2/3)

[Everdij&Blom, 2010] M.H.C. Everdij and H.A.P. Blom. Bisimulation relations between automata, stochastic differential equations and Petri nets. In M. Bujorianu and M. Fisher, editors, *Proceedings workshop on Formal Methods for Aerospace (FMA), Electronic Proceedings in Theoretical Computer Science (EPTCS)*, Vol. 20, 2010, pp. 1–15.

[Everdij, 2010] M.H.C. Everdij, Compositional modelling using Petri nets with the analysis power of stochastic hybrid processes, PhD Thesis, Twente University, Enschede, June 2010.

[Prandini&Hu, 2006] M. Prandini, J. Hu. A stochastic approximation method for reachability computations. Eds: H.A.P. Blom, J. Lygeros, Stochastic Hybrid Systems, Theory and safety critical applications, Springer, Berlin, July 2006, pp. 107-139.

[Abate et al., 2006] A. Abate, S. Amin, M. Prandini, J. Lygeros, S. Sastry, Probabilistic reachabiliy for discrete time stochastic hybrid systems, Proc. IEEE Conference on Decision and Control, December 2006, pp. 258-263.

[Cerou et al. 2002] F. Cerou, P. Del Moral, F Legland, P. Lezaud, Genetic genealogical models in rare event analysis, Publications du Laboratoire de Statistiques et Probabilites, Toulouse III, 2002

[Cerou et al. 2005] F. Cerou, P. Del Moral, F Legland, P. Lezaud, Limit theorems for the multi-level splitting algorithms in the simulation of rare events, Proc. 2005 Winter Simulation Conf., Orlando, USA.

- References (3/3)

[Krystul&Blom, 2005] J. Krystul, H.A.P. Blom, Sequential Monte Carlo simulation of rare event probability in stochastic hybrid systems, Proc. 16th IFAC World congress, July 4-8, 2005.

[Krystul&Blom, 2006] J. Krystul, H.A.P. Blom, Sequential Monte Carlo simulation for the estimation of small reachability probabilities for stochastic hybrid systems, Proc. IEEE-EURASIP Int. Symp. on Control, Communications and Signal Processing (ISCCSP2006), March 13-15, 2006, Marrakech, Morocco.

[Blom,Bakker&Krystul, 2007] H.A.P. Blom, G.J. Bakker, J. Krystul, Probabilistic reachability analysis for large scale stochastic hybrid systems, Proc. IEEE Conf. on Decision and Control, 12-14th December 2007, New Orleans, LA, USA, pp. 3182-3189.

[Blom,Bakker&Krystul, 2009] H.A.P. Blom, G.J. Bakker, J. Krystul, Rare event estimation for a large-scale stochastic hybrid system with air traffic application, Eds: G. Rubino and B. Tuffin, Rare event simulation using Monte Carlo methods, J.Wiley, 2009, pp. 193-214.

[Blom et al., ATC-Q, 2009] H.A.P. Blom, B. Klein Obbink, G.J. Bakker, Simulated safety risk of an uncoordinated airborne self separation concept of operation, ATC-Quarterly, Vol. 17 (2009), pp. 63-93.

[Bujorianu et al., 2005] M.L. Bujorianu, J. Lygeros, and M.C. Bujorianu. Different approaches on bisimulation for stochastic hybrid systems. In M. Morari and L. Thiele, editors, *Proceedings 8th Hybrid Systems: Computation and Control (HSCC2005), Zürich, Switzerland*, *Lecture notes in computer science (LNCS)*, Volume 3414, 2005, pp. 198–214.