

ПРОЦЕСС ОЦЕНКИ БЕЗОПАСНОСТИ АТ С ПРИМЕНЕНИЕМ МОДУЛЕЙ RAM COMMANDER

Контроль отказобезопасности

- говоря о отказобезопасности систем, следует понимать, что это свойство технической системы при отказе некоторых её частей переходить в режим работы, не представляющий опасности для людей, окружающей среды или материальных ценностей, а также позволяющее безопасно завершить полет
- на современном уровне развития авиационной науки и техники невозможно создать абсолютно безотказные технические системы

Постановка проблемы

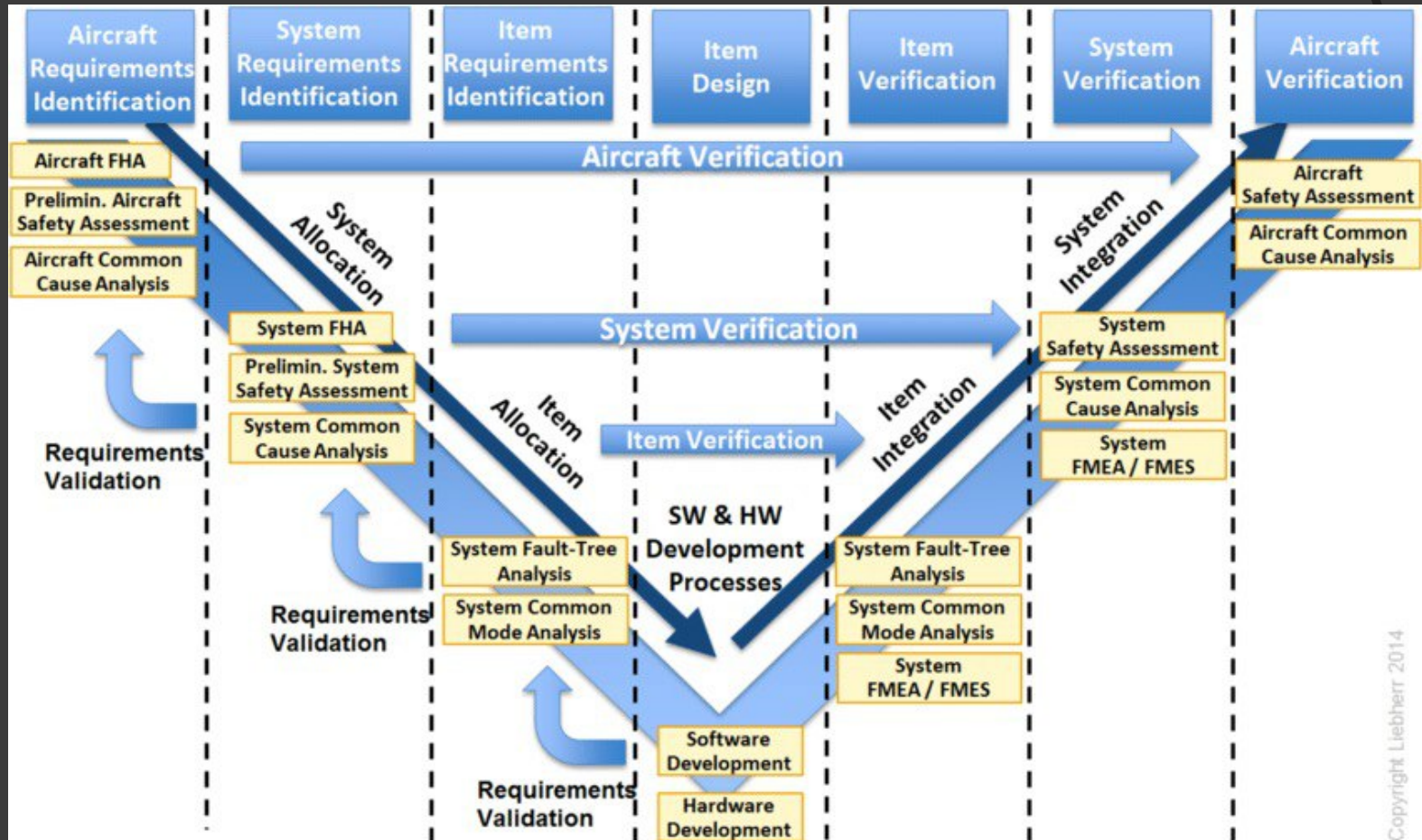
- важной проблемой при проектировании АТ является полнота оценки уровня отказобезопасности

Модель обеспечения безопасности

- Последовательность разработки системы «сверху вниз», начиная с определения требуемой функции воздушного судна, обеспечивает удобную концептуальную модель процесса разработки АТ



Документ ARP 4754A



Задачи отказобезопасности

Приоритетными задачами является определение:

- перечня функций систем АТ
- перечня потенциально возможных нарушений функции (отказных состояний, функциональных отказов, видов отказов системы) авионики
- последствий каждого ФО для пассажиров, экипажа и ВС в целом
- оценка степени опасности (уровня критичности, степени риска) для каждого из функциональных отказов

Облик системы

- Особенностью подхода к формированию модели является выделение технического облика системы
- В результате этапа разработки архитектуры появляется описание системы с детализацией до уровня элементов, а также производные требования, определяющие интерфейсы системы, ограничения и уровень интеграции между функциями

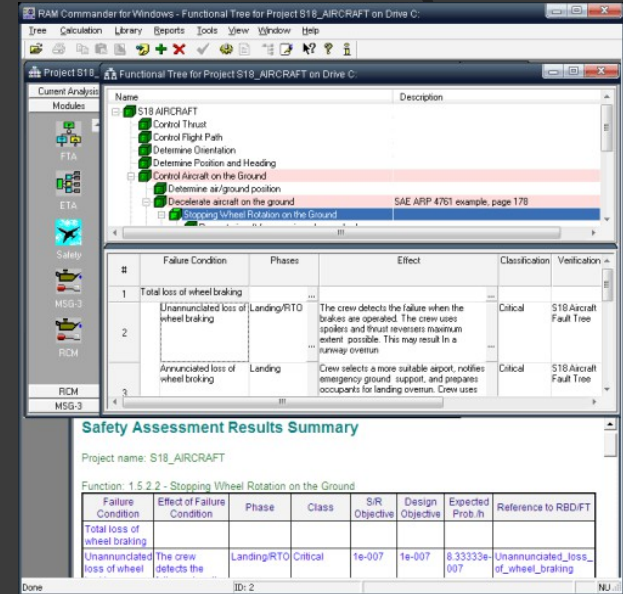
Применение RAM Commander

- RAM Commander сочетает инновационный подход, точность вычислений, удобство использования. RAM Commander решает сразу целый список инженерных задач по надежности электронных, электро-механических и механических систем. RAM Commander является модульным ПО, которое предоставляет заказчикам гибкость в постепенном добавлении модулей к пакету инструментов в зависимости от требований проекта и выделенных денежных средств



Основные процессы оценки безопасности

- ПО по анализу отказобезопасности - это универсальный инструмент, который выполняет требования и задачи SAE ARP4761, MIL-STD-882 и других стандартов.
- Процесс анализа отказобезопасности крайне важен для постановки целей отказобезопасности анализируемой системы и выяснения, соответствует ли выполнение анализа этим целям. Процесс анализа отказобезопасности является итерационным по своей сути.

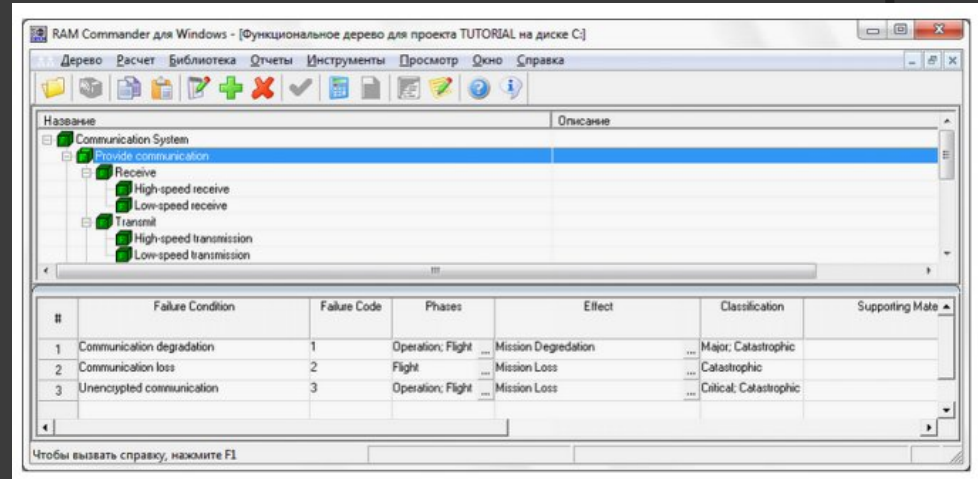
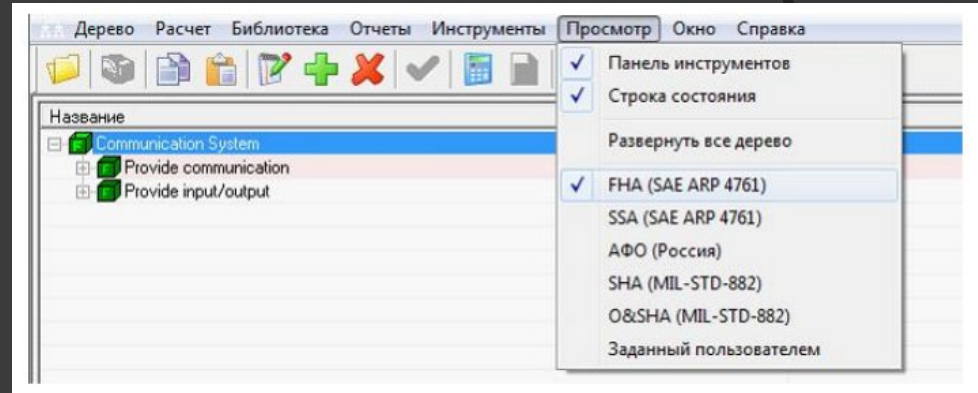


Основные процессы оценки безопасности

- Процесс оценки безопасности включает в себя применение следующих методов:
- Оценка функциональных опасностей (functional hazard assessment – FHA)
- Анализ общих причин (common cause analysis – CCA)
- Предварительная оценка безопасности (preliminary system safety assessment – PSSA)
- Анализ/сводка видов и последствий отказов (failure modes and effects analysis/summary – FMEA/FMES)
- Оценка безопасности (system safety analysis – SSA)

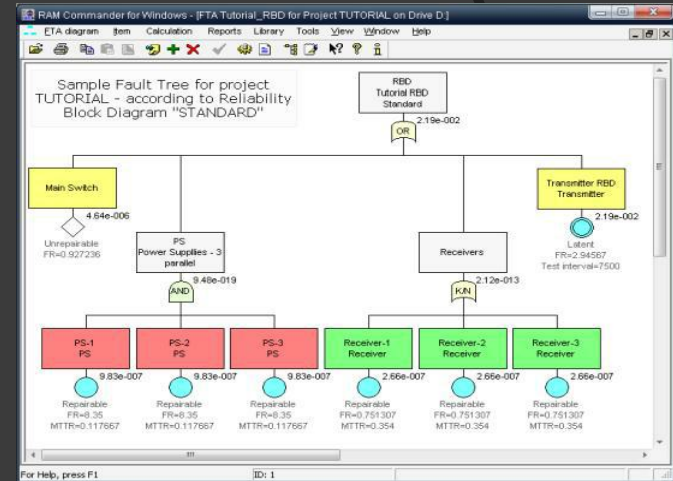
Модуль Safety

- В соответствии с руководством 4761 приоритетной задачей оценки безопасности АТ является оценка функциональной опасности (ФНА)
- Целью ФНА является рассмотрение функций на наиболее приемлемом уровне, выявление и классификация возникающих отказных состояний вследствие как потери функций, так и неправильного выполнения.
- ФНА должна выявлять отказные состояния для каждого этапа полета, если воздействие отказа и классификация состояния изменяется от одного этапа к другому



Fault tree analysis (FTA)

- Анализ деревьев отказов представляет графический способ презентации логической структуры с отображением нежелательных событий (отказов) и их причин.
- FTA представляет возможность сосредоточиться на важном событии, таком как критическая угроза безопасности, и работать над тем, чтобы уменьшить его вероятность и последствия.
- Получившаяся в итоге диаграмма дерева отказов это графическая репрезентация цепи событий в вашей системе или процессе, созданная на основе событий и конфигураций логических элементов.



Возможно два типа анализа с помощью ПО анализа деревьев отказов

Количественный анализ

Качественный анализ

FTA - Minimum Cut Sets
 Project name: TUTORIAL
 FTA: Tutorial
 Top event: Communication system general failure
 Q mean=2.31921e-006
 MCS count: 8
 MCS max.order: 2

N	Q mean	%	Order	Event 1	Event 2
1	9.82518e-007	42.4	1	PS	
2	3.78288e-007	16.3	1	Mother Board - Memory Fail	
3	3.26156e-007	14.1	1	HardDrive	
4	2.65963e-007	11.5	1	Receiver failure	
5	2.21943e-007	9.6	1	Antenna failure	
6	1.13333e-007	4.9	1	Keyboard	
7	2.7264e-008	1.2	1	Mother Board - CPU Fail	
8	3.75081e-009	0.2	2	Alternative transmitter failure	Transmitter failure

Minimal Cut Sets distribution by order

Order	Number of MCS
1	7
2	1

FTA - Importance & Sensitivity Analysis
 Project name: TUTORIAL
 FTA: sample
 Top event: Information system failure
 Q mean=0.00218462

N	Code	Occurrence	Q mean	FV Imp.	FC	RDF	RIF	Sens. high	Sens. low	Sensitivity
1	DB engine files absent	1	1e-006	0.000458	0.000457	1.00046	457.748	0.0021926	0.002194	1.00462
2	DB engine registry record is bad	1	1e-006	0.000458	0.000457	1.00046	457.748	0.0021926	0.002194	1.00462
3	Installation files bad	1	3e-005	0.0137324	0.0137032	1.01389	457.748	0.002454	0.002158	1.13735
4	License	3	0.004	0.0704609	0.0703462	1.07567	18.3988	0.003567	0.0020463	1.74334
5	Plug absent	1	0.03	0.0546295	0.0548165	1.058	2.77238	0.003262	0.002077	1.57684
6	Plug driver failure	1	0.008	0.0146479	0.0149167	1.01483	2.81242	0.002472	0.002156	1.14663
7	Port failure	1	0.0005	0.000915	0.000914	1.00091	2.82607	0.002203	0.002183	1.00805
8	Required ActiveX not registered	1	0.001	0.467746	0.457203	1.84231	457.748	0.0111739	0.001286	8.89104
9	Software registry records bad	1	0.001	0.467746	0.457203	1.84231	457.748	0.0111739	0.001286	8.89104

Notes:
 Occurrence - number of occurrences of the basic event in all minimal cut sets
 FV Importance - Fussell-Vesely Importance (FV = Q of MCS which contains the basic event / Q of all MCS)
 FC - Fractional Contribution of Basic Event (1-1/RDF)
 RDF - Risk Decrease Factor
 RIF - Risk Increase Factor
 Sensitivity - Sensitivity Value, calculated with sensitivity factor=10

Failure mode, effects, and criticality analysis (FMECA)

- Анализ видов, последствий и критичности — это логическое продолжение и во многих случаях неотъемлемая часть анализа безопасности.
- Модуль FMECA подходит как для оборудования, так и для функциональных подходов к FMECA, полностью соответствует требованиям MIL-STD-1629, коммерческим стандартам и поддерживает анализ функциональной безопасности согласно IEC 61508.

Project TUTORIAL on Drive C:

Ref Des.	ID	Name	Qty	Opt. FR [10 ⁻⁶]	Status	MTBF	Temp.
TUTORIAL	1	Communication System	1	187.0768		5345.398	35.0
Communic	1	COMM001	1	100.2550		9974.567	35.0
Main Switch	1	SW986	2	8.7416		1.1E+005	45.0
Switching	1	---	1	3.9690		2.5E+005	35.0
Scrambling	2	---	1	0.3819		2.6E+006	35.0
Receiver	2	RC004	10	82.8214		1.2E+004	45.0
Transmitter	3	TR987-001	1	0.3419		2.9E+006	40.0
PS	4	Power Supply	1	8.3500		1.2E+005	40.0
Control	2	Control Unit	1	75.4953		1.3E+004	25.0
Monitor	1	MON001	1	8.0000		1.3E+005	25.0
Keyboard	2	KB003	1	17.0000		6.9E+004	25.0
Systemlock	3	MS555	1	5.1E+00		2.1E+001	25.0
Pedestal	3	PO001	1	11.3265		8.9E+004	35.0
Antenna	1	ANT1555	1	6.6583		1.5E+005	35.0
Motor	2	MDT378	1	4.5000		2.2E+005	35.0
Bearing	3	B0856	1	0.1682		5.9E+006	35.0

#	FM	Description	IDN	NHE	Description	Beta	EE	Description	Beta	Severity
1		Error in Data processing	1.2		Wrong System Control	1.000		Communication Degradation	0.800	III
2		No additional software loading						Maintenance Degradation	0.200	IV
3		No system initialization	1.2		No effect	1.000		Performance Degradation	1.000	IV
4		No new drivers data	1.2		No version changing	0.500		Maintenance Degradation	1.000	IV
5		No data processing	1.2		No initial system testing	0.500		Maintenance Degradation	1.000	IV
6			1.2		Communication System Control	1.000		Communication Loss	1.000	II

Анализ контролепригодности

- главные характеристики контролепригодности — это охват ВИТ/обнаружения и локализация неисправности. Они могут быть вычислены для любого уровня технического обслуживания (организационный уровень, промежуточный уровень, уровень базы технического обслуживания) и для определенных методов обнаружения (ВИТ, ВИТЕ, внешняя испытательная аппаратура и др.). Эффективность метода контроля и индикация определены для каждого метода контроля или группы методов контроля.

Coverage per Item Report for Project TUTORIAL Drive C:

Coverage per Item

Project name: TUTORIAL
Phase: Operation
For Severity : Catastrophic, Critical, Marginal, Minor
For Classification :
For Level of Replace : Organizational, Intermediate, Depot, Supplier, Manufacturer
For Test Level : Organizational (O), Intermediate (I), Depot (D), Supplier (S), Manufacturer (M)
For Test Type : All Test Types
For Tests : All Tests

Assembly Name: TUTORIAL, IDN: 1, Description: Communication System

Coverage	IDN	Name	Item Coverage	Detected FR (*E-5) (Single Item)	Detected FR (*E-5) (Total Qty)	Total FR (*E-6) (Total Qty)
0.752	1.1	Communic	0.897	89.557	89.557	99.852
	1.1.1	Main Switch	0.266	1.110	2.219	8.338
	1.1.1.1FB	Switching	0.300	0.555	1.110	3.698
	1.1.1.2FB	Scrambling	0.000	0.000	0.000	0.471
	1.1.2	Receiver	1.000	8.282	82.821	82.821
	1.1.3	Transmitter	1.000	0.342	0.342	0.342
	1.1.4	PS	0.500	4.175	4.175	8.350
	1.2	Control	0.557	36.489	36.489	65.485
	1.2.1	Monitor	0.000	0.000	0.000	8.000

Связь модулей RAM Commander

The screenshot displays the RAM Commander interface for a project named 'TUTORIAL_MMEL on Drive C'. It is divided into several key sections:

- Current Analysis:** A table listing components such as 'Air Conditioning System', 'BLEED SYSTEM', 'WING ICE PROTECTION SYSTEM', 'ENVIRONMENTAL CONTROL SYST.', 'FLOW CONTROL VALVE', 'PACK INLET FLOW SENSOR L', 'PACK INLET FLOW SENSOR R', and 'PACK INLET PRESSURE SENSO...'.
- FR Table:** A table with columns for ID, Name, Qty, Op. FR, and Status. It lists Functional Requirements (FR) like 'Valve always indicated NFC' and 'Valve always indicated FC'.
- Functional Tree:** A hierarchical tree showing the structure of the analysis, including 'AIRC_EN_1', 'Air conditioning system', and 'Cabin pressure control system (CPCS)'.
- Failure Condition Table:** A table with columns for Failure Condition, Phases, Effect, Classification, Assessment, Expected probability/hour, and Objective probability/hour. It lists conditions like 'Annunciated total absence of air supply to - air conditioning system...'.
- Fault Tree Diagram:** A diagram showing the relationship between failure events. The top event is '21_A11111311_L Component failure leading to pack closure 1 /2' with a probability of 2.10e-005. This event is linked to an OR gate, which is connected to five basic events:
 - CDTS 1 L: Erroneous information on one channel (Unrepairable, FR=0.6, 2.34e-006)
 - CDTS 2 L: Erroneous information on both channels (Unrepairable, FR=1.389, 5.42e-006)
 - CDTS 4 L: Loss of information on both channels (Unrepairable, FR=0.0676, 2.64e-007)
 - FCV 6 L FLOW CONTROL VALVE Valve always indicated FC (Unrepairable, FR=0.641025, 4.67e-006)
 - PIFS 1 L PACK INLET FLOW SENSOR L Leak (Unrepairable, FR=0.04, 1.56e-007)

Red annotations highlight the connections between these modules:

- 'FR, MTR, Alpha' points to the FR table and the Assessment column of the Failure Condition table.
- 'Probability' points to the Expected probability/hour column of the Failure Condition table and the basic events in the fault tree.

Достоинства RAM Commander

- Выполняет количественный и качественный анализ отказобезопасности:
- Формирование и проверка требований отказобезопасности
- Идентификация всех характерных отказных состояний
- Рассмотрение всех значимых комбинаций отказов, которые являются причиной отказных состояний

Работа в условиях санкций

- Продукт доступен в России
- Удовлетворяет всем требованиям стандартов проектирования современной авионики

Наши заказчики



Заключение

- Благодаря вышеописанным действиям программный комплекс позволяет формировать доказательную документацию по отказобезопасности в соответствии с рядом отечественных и зарубежных правил

Благодарю за внимание!