СОФТВЕР ЛАБС
НАДЁЖНОСТЬ И ОТКАЗОБЕЗОПАСНОСТЬ

ПРОЦЕСС ОЦЕНКИ БЕЗОПАСНОСТИ АТ С ПРИМЕНЕНИЕМ МОДУЛЕЙ RAM COMMANDER

Контроль отказобезопасности

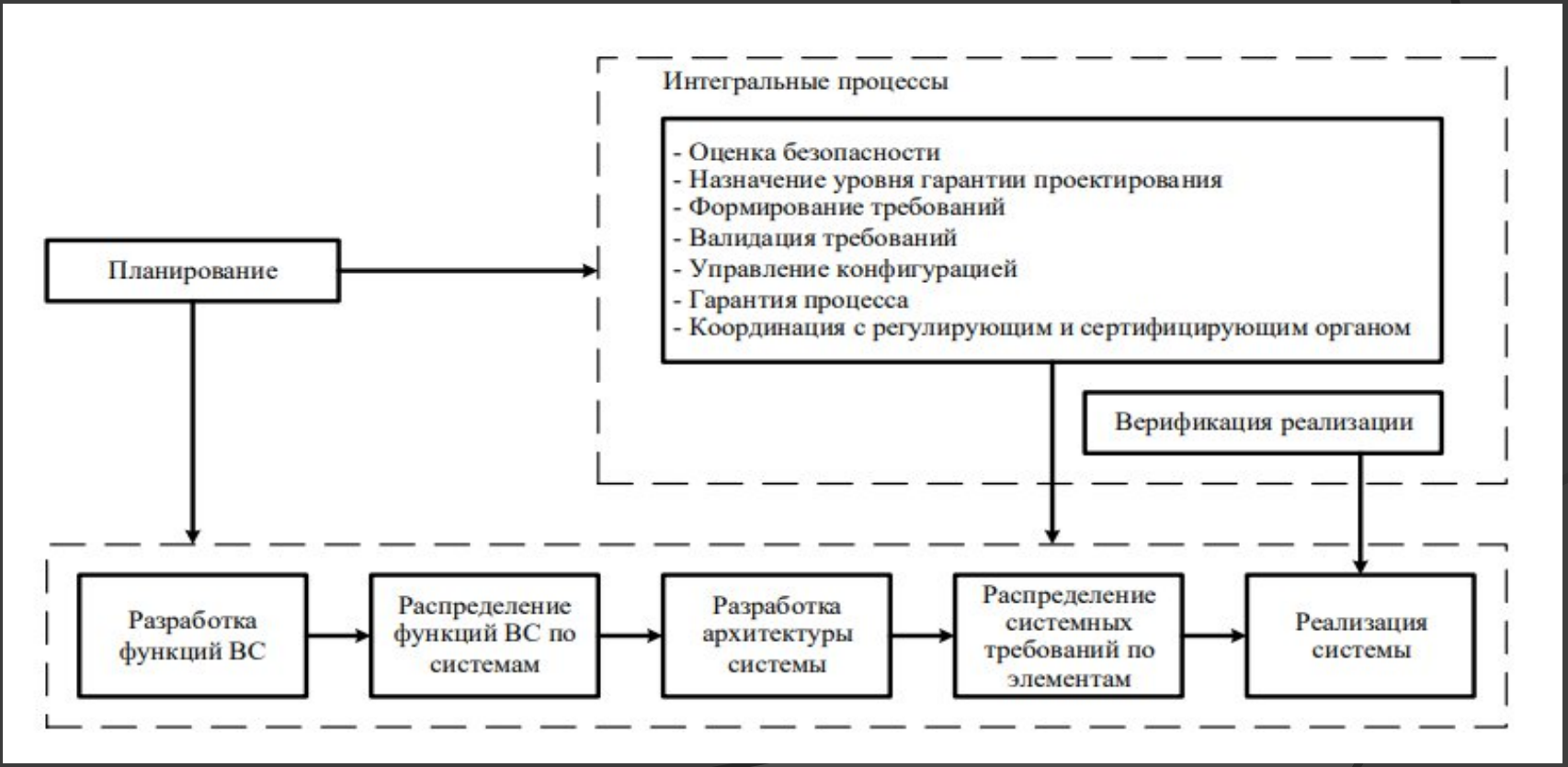
- говоря о отказобезопасности систем, следует понимать, что это свойство технической системы при отказе некоторых её частей переходить в режим работы, не представляющий опасности для людей, окружающей среды или материальных ценностей, а также позволяющее безопасно завершить полет
- на современном уровне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

Постановка проблемы

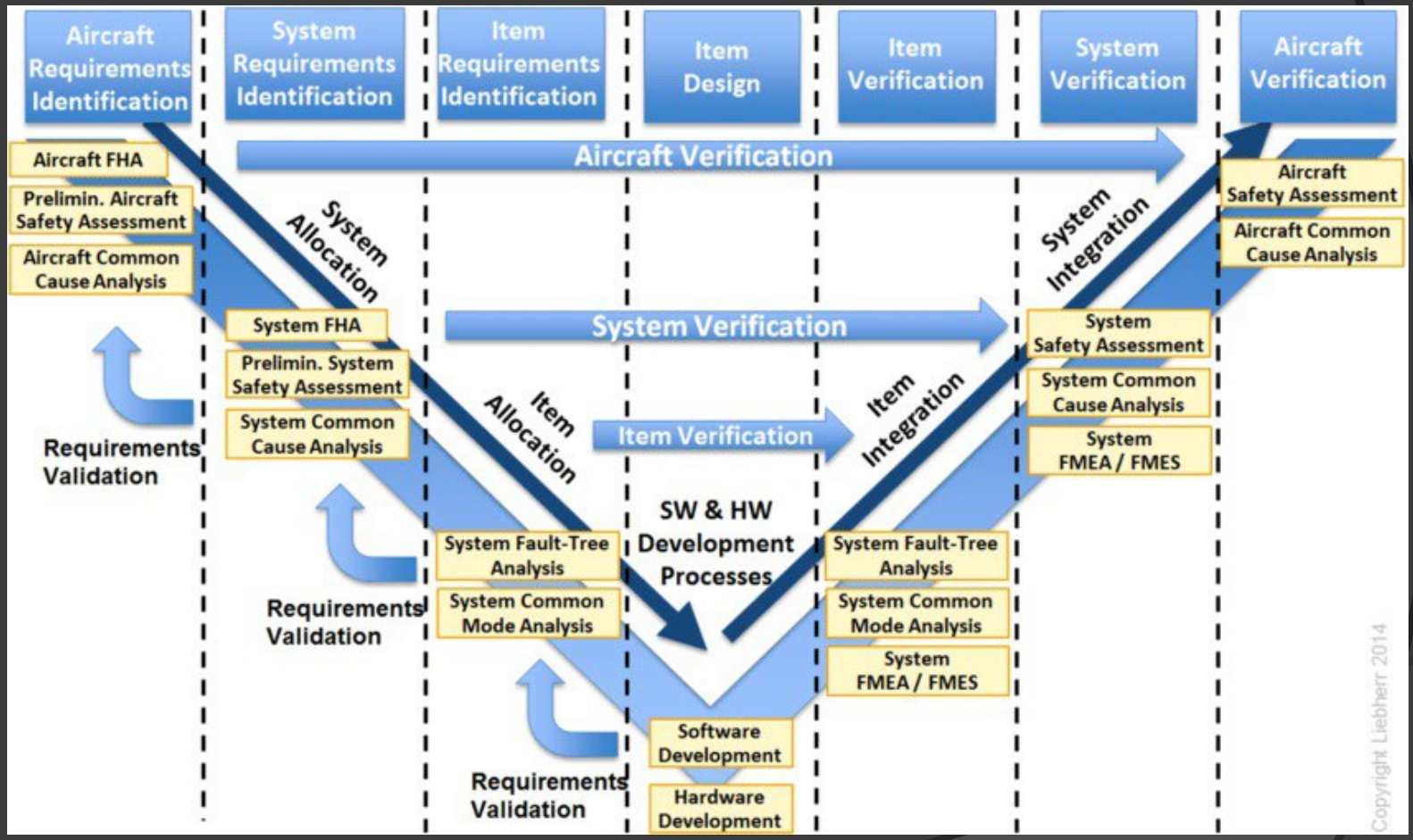
- важной проблемой при проектировании АТ является полнота оценки уровня отказобезопасности

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:

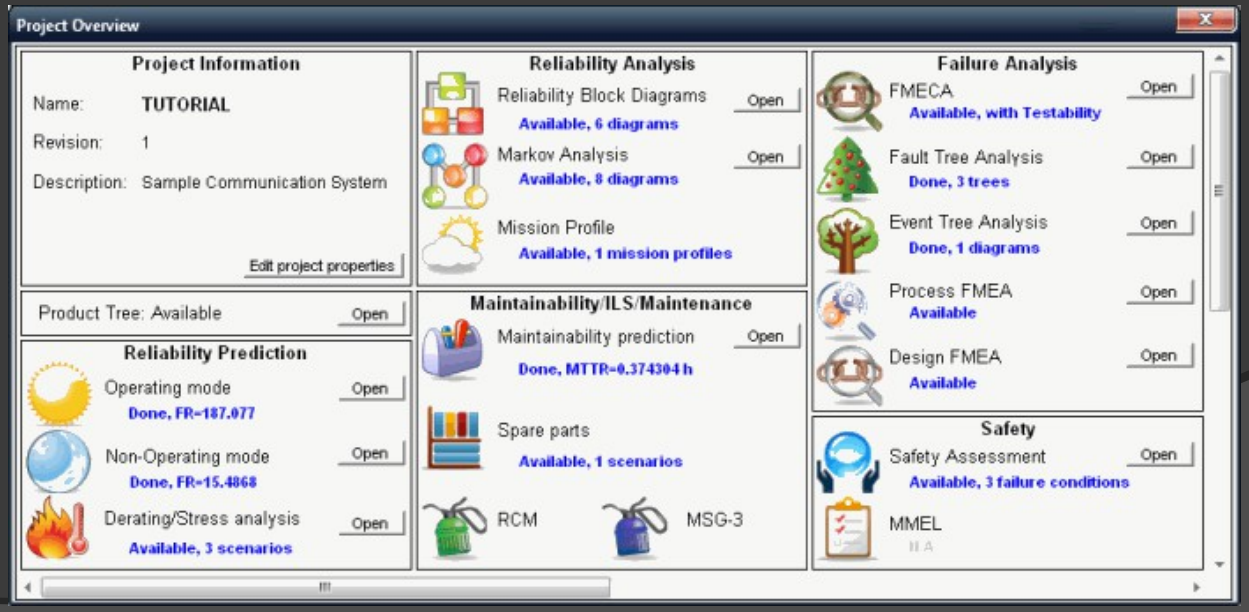
- перечня функций систем АТ
- перечня потенциально возможных нарушений функции (отказных состояний, функциональных отказов, видов отказов системы) авионики
- последствий каждого ФО для пассажиров, экипажа и ВС в целом
- оценка степени опасности (уровня критичности, степени риска) для каждого из функциональных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

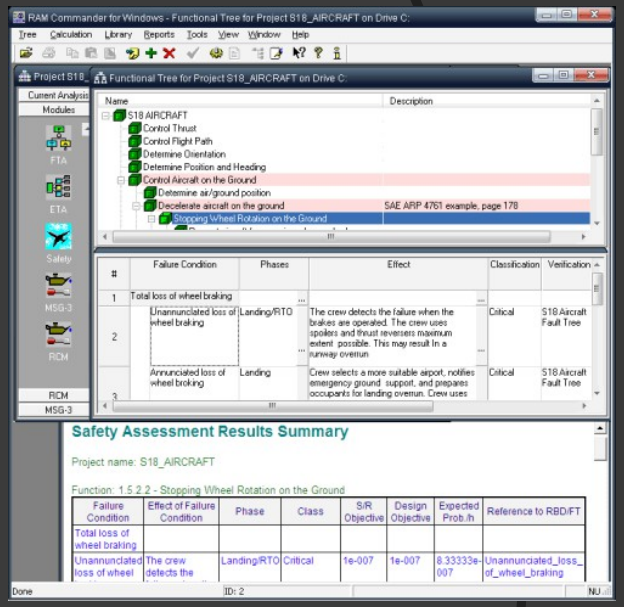
Применение RAM Commander

- 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.

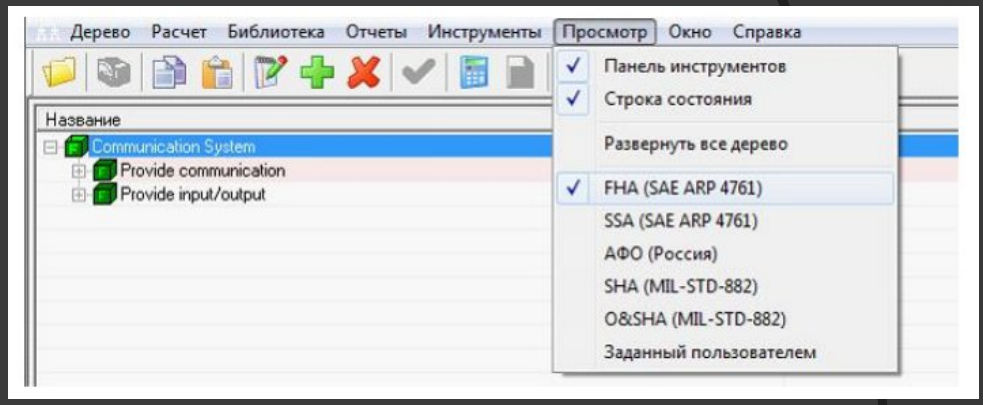


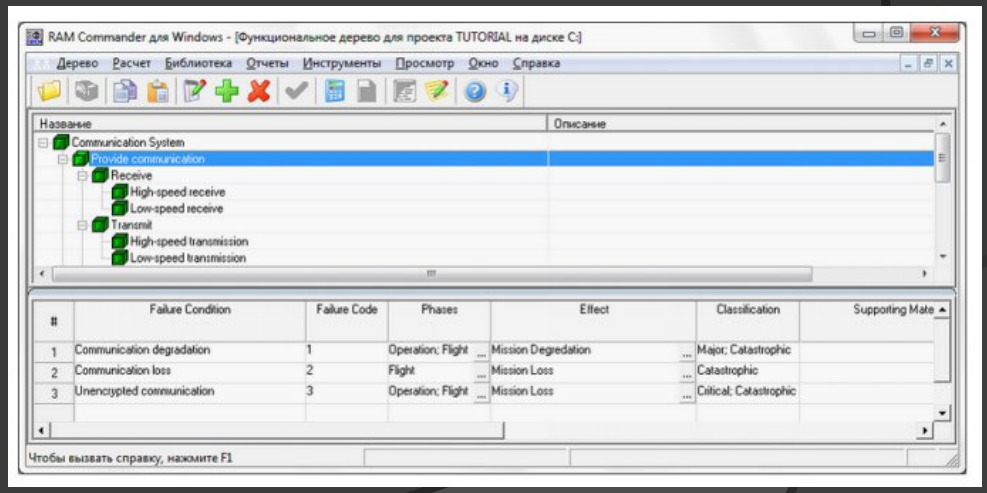
Основные процессы оценки безопасности

- 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

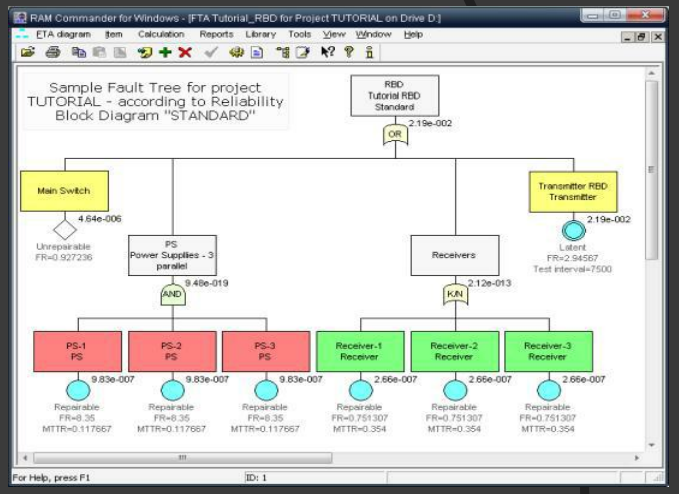
- В соответствии с руководством 4761 приоритетной задачей оценки безопасности АТ является оценка функциональной опасности (FHA)
- Целью FHA является рассмотрение функций на наиболее приемлемом уровне, выявление и классификация возникающих отказных состояний вследствие как потери функций, так и неправильного выполнения.
- FHA 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

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

Качественный анализ

FTA - Importance & Sensitivity Analysis

Project name: TUTORIAL
FTA: sample
Top event: Information system failure
Q mean=0.00218462

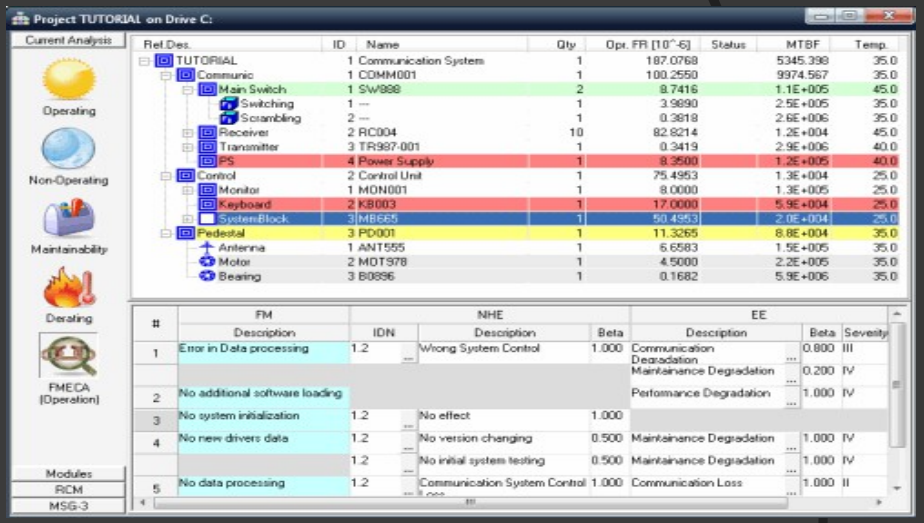
N	Code	Occurrence	Q mean	FV Imp.	FC	RDF	RIF	Sens. high	Sens. low	Sensitivity
1	DB engine files absent	1	1e-006	0.000458	0.000457	1.00046	457.746	0.0021936	0.002184	1.00452
2	DB engine registry record is bad	1	1e-006	0.000458	0.000457	1.00046	457.746	0.0021936	0.002184	1.00452
3	Installation files bad	1	3e-005	0.0137324	0.0137032	1.01389	457.746	0.002454	0.002168	1.13735
4	License	3	0.004	0.0704909	0.0703482	1.07567	18.3988	0.003567	0.0020463	1.74334
5	Plug absent	1	0.03	0.0549295	0.0548165	1.058	2.77238	0.003262	0.002077	1.57084
6	Plug driver failure	1	0.008	0.0146479	0.0146167	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	1.00905
8	Required ActiveX not registered	1	0.001	0.457746	0.457203	1.84231	457.746	0.0111739	0.001286	8.69104
9	Software registry records bad	1	0.001	0.457746	0.457203	1.84231	457.746	0.0111739	0.001286	8.69104

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
RDF - Risk Increase Factor
Sensitivity - Sensitivity Value, calculated with sensitivity factor=10

Failure mode, effects, and criticality analysis (FMECA)

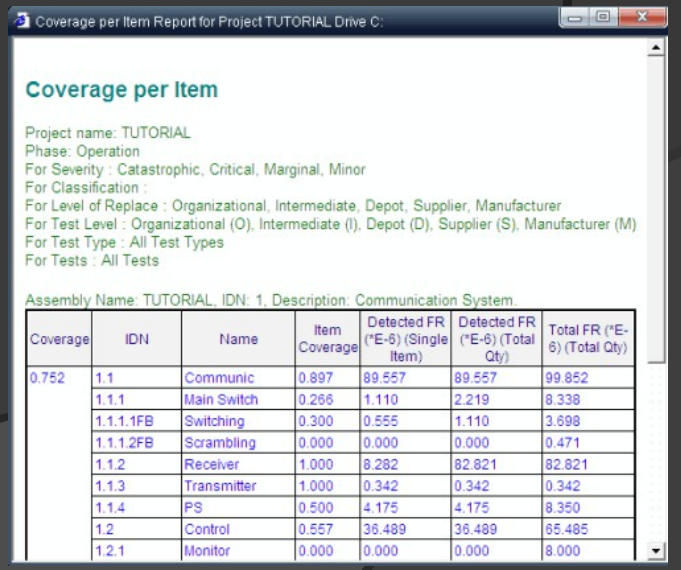
СОФТВЕР ЛАБС
НАДЁЖНОСТЬ И ОТКАЗОБЕЗОПАСНОСТЬ

- 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.

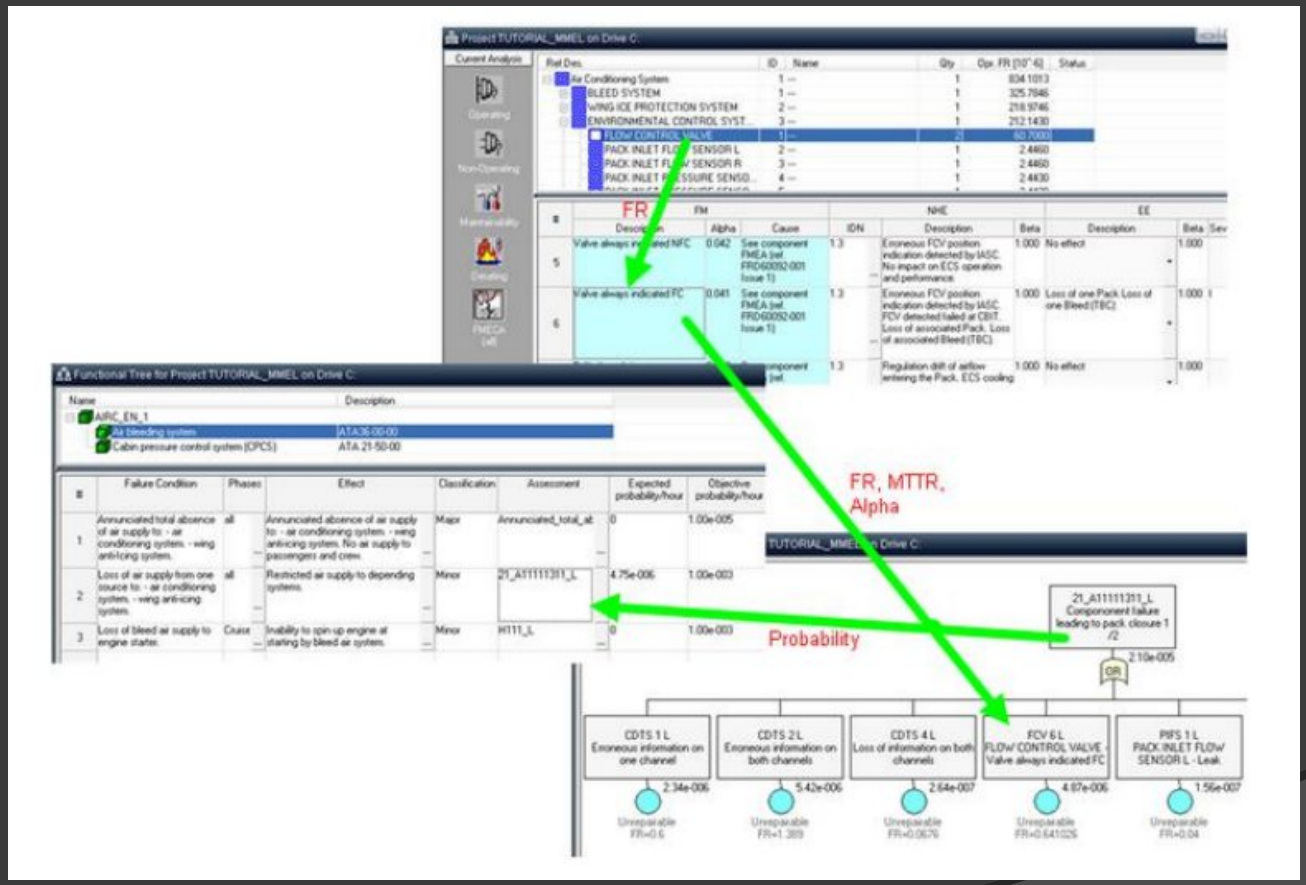


- **Анализ контролепригодности**

- главные характеристики контролепригодности – это охват BIT/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 (BIT, BITE, внешняя испытательная аппаратура и др.). Эффективность метода контроля и индикация определены для каждого метода контроля или группы методов контроля.



Связь модулей RAM Commander



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

СОФТВЕР ЛАБС
НАДЁЖНОСТЬ И ОТКАЗОБЕЗОПАСНОСТЬ

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

СОФТВЕР ЛАБС
НАДЁЖНОСТЬ И ОТКАЗОБЕЗОПАСНОСТЬ

Благодарю за внимание!