Анализ видов и последствий отказов на основе архитектурных моделей программно-аппаратных систем

С.Зеленов, Д.Буздалов,
А.Угненко, А.Хорошилов

Институт системного программирования им. В.П. Иванникова РАН (ИСП РАН)

Жизненный цикл разработки

- Требования
- Проектирование
- Реализация
- Тестирование

Причины отказов

- 40-45% - ошибки проектирования,
- 20% - ошибки при производстве,
- 30% - неправильная эксплуатация,
- 5-10% - естественный износ и старение

Глазунов Л.П., Грабовецкий В.П., Щербаков О.В. Основы надежности автоматических систем управления. // Л.: Энергоатомиздат, Ленинградское отделение, 1984, - 208 с., ил.

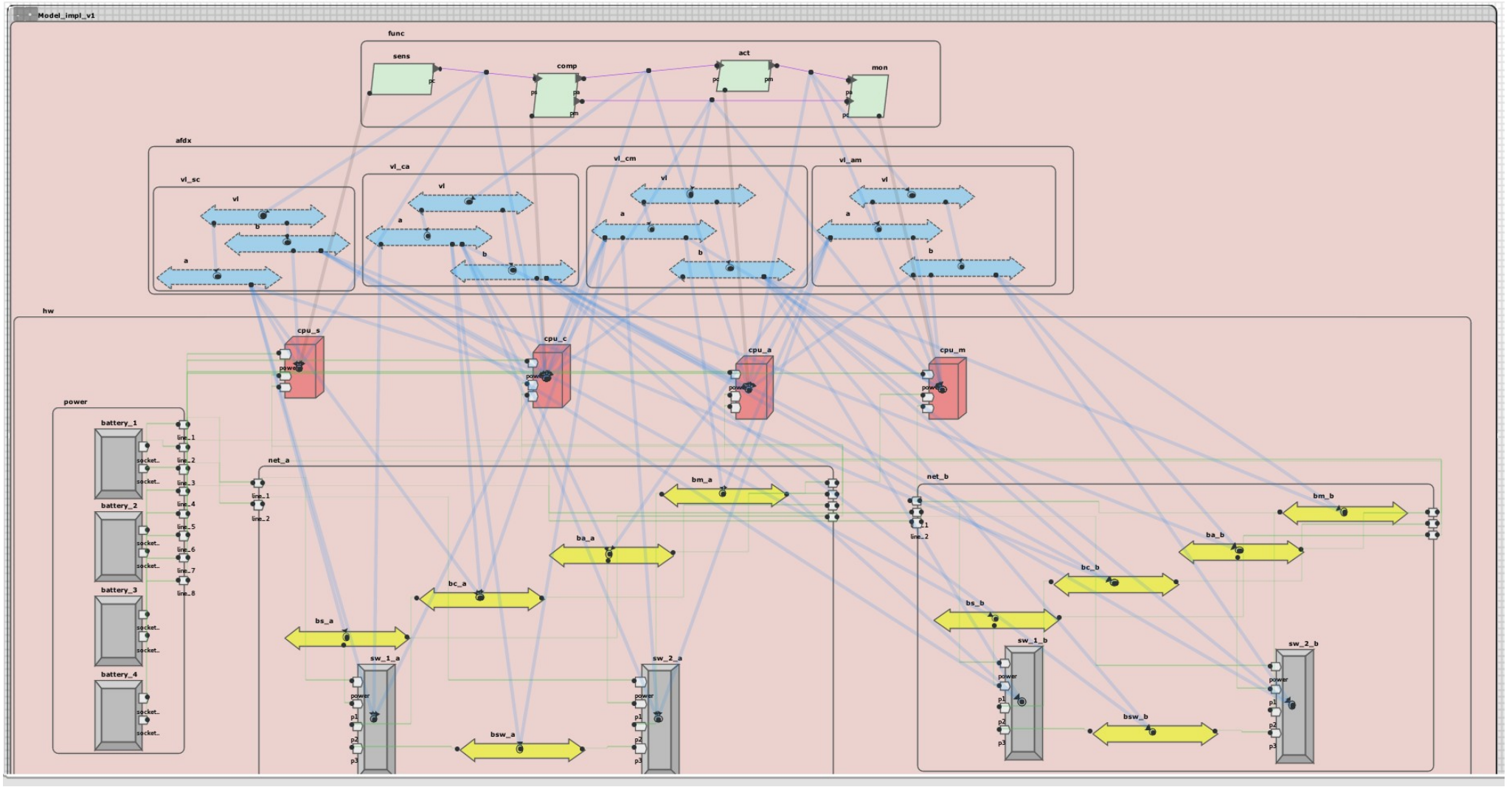
Ранняя валидация

- Требования
- Проектирование
  - **Ранняя валидация**
- Реализация
- Тестирование

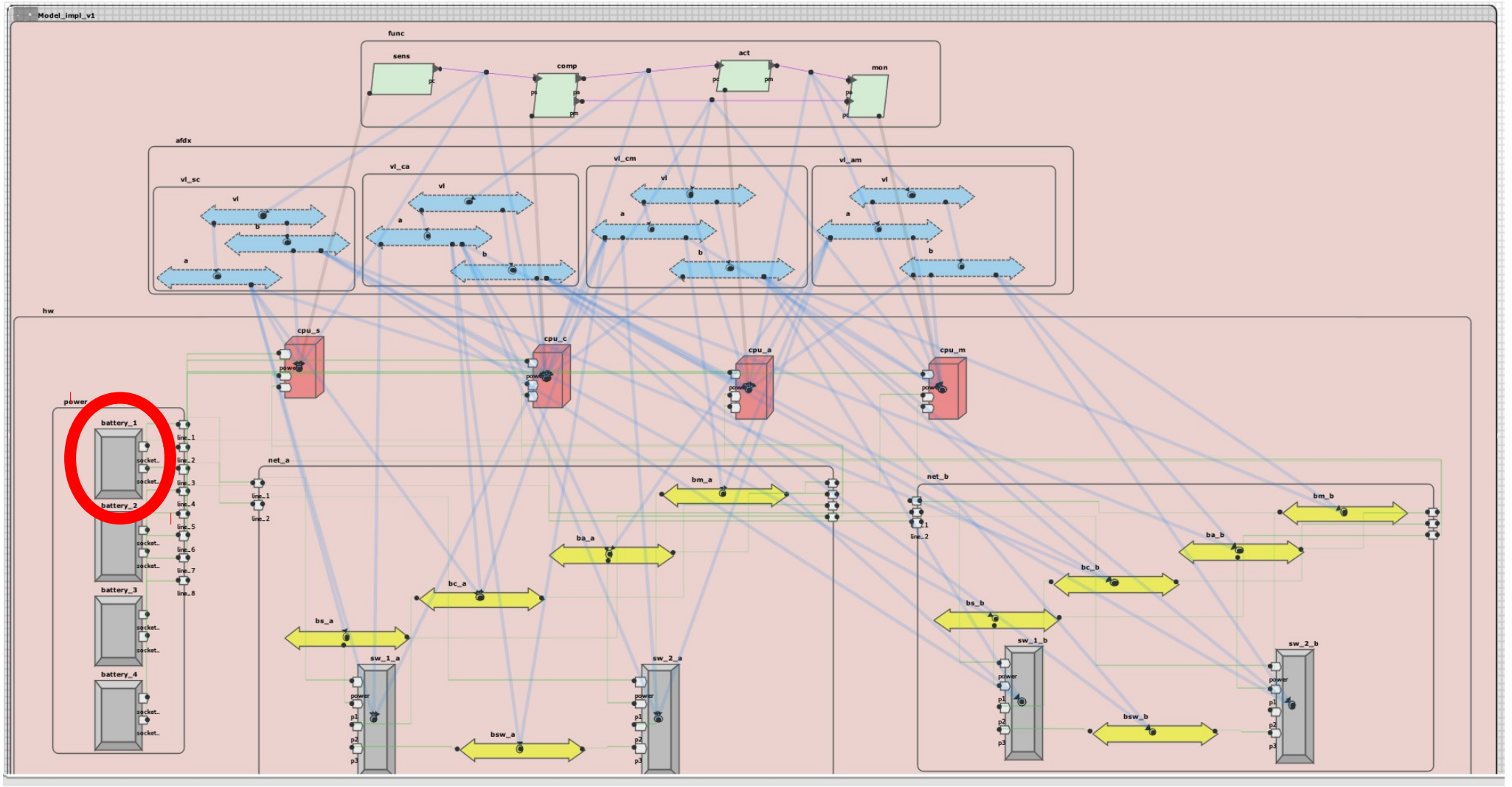
Анализ видов и последствий отказов (Failure Mode and Effect Analysis, FMEA)

- SAE International standard ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996. http://standards.sae.org/arp4761/.
- Анализ надежности
- Обязательно при проектировании авиационных систем
- “Снизу вверх”
  - Отказ компонента => последствия для системы

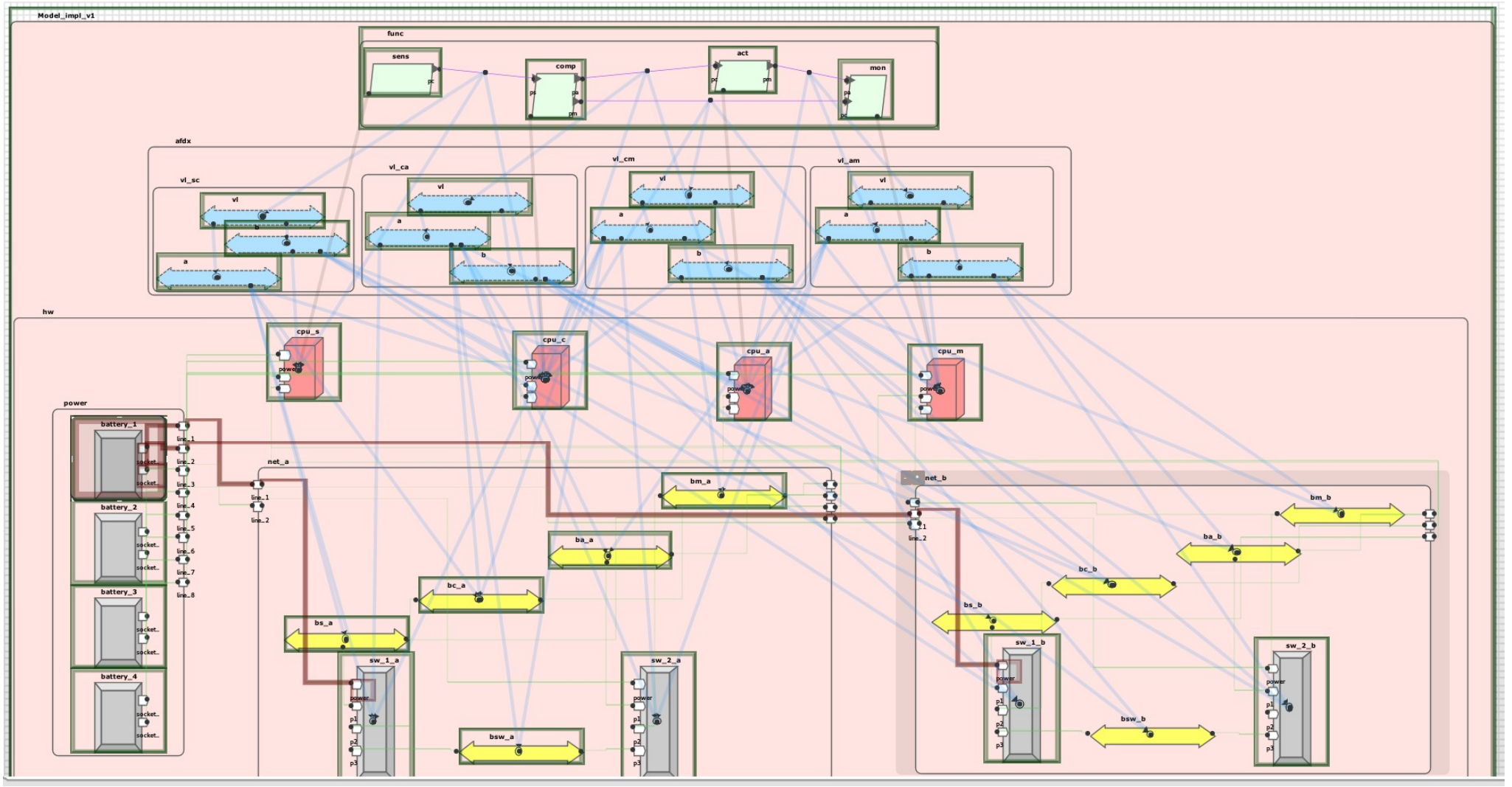
Пример: система



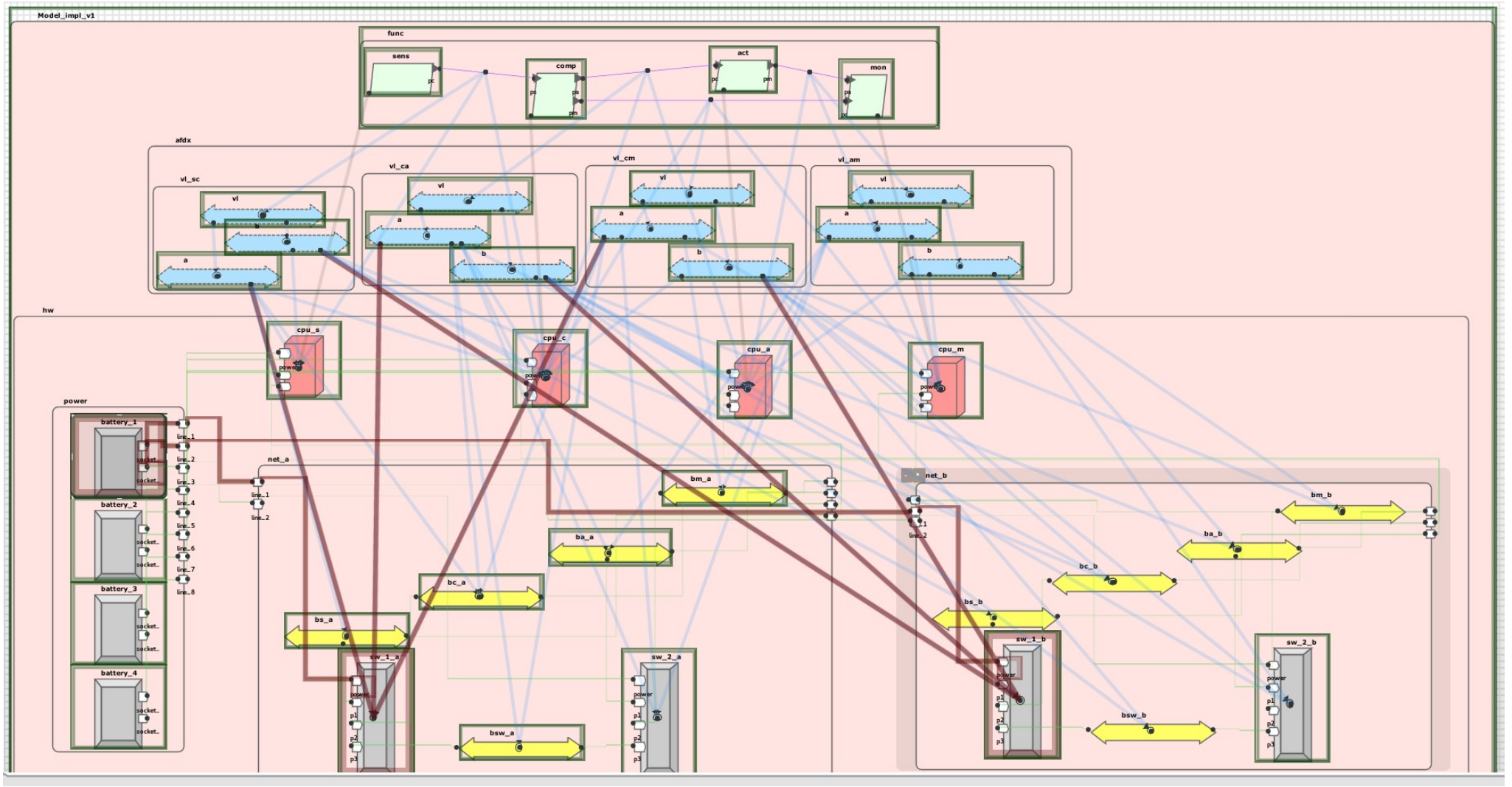
Пример: отказ компонента



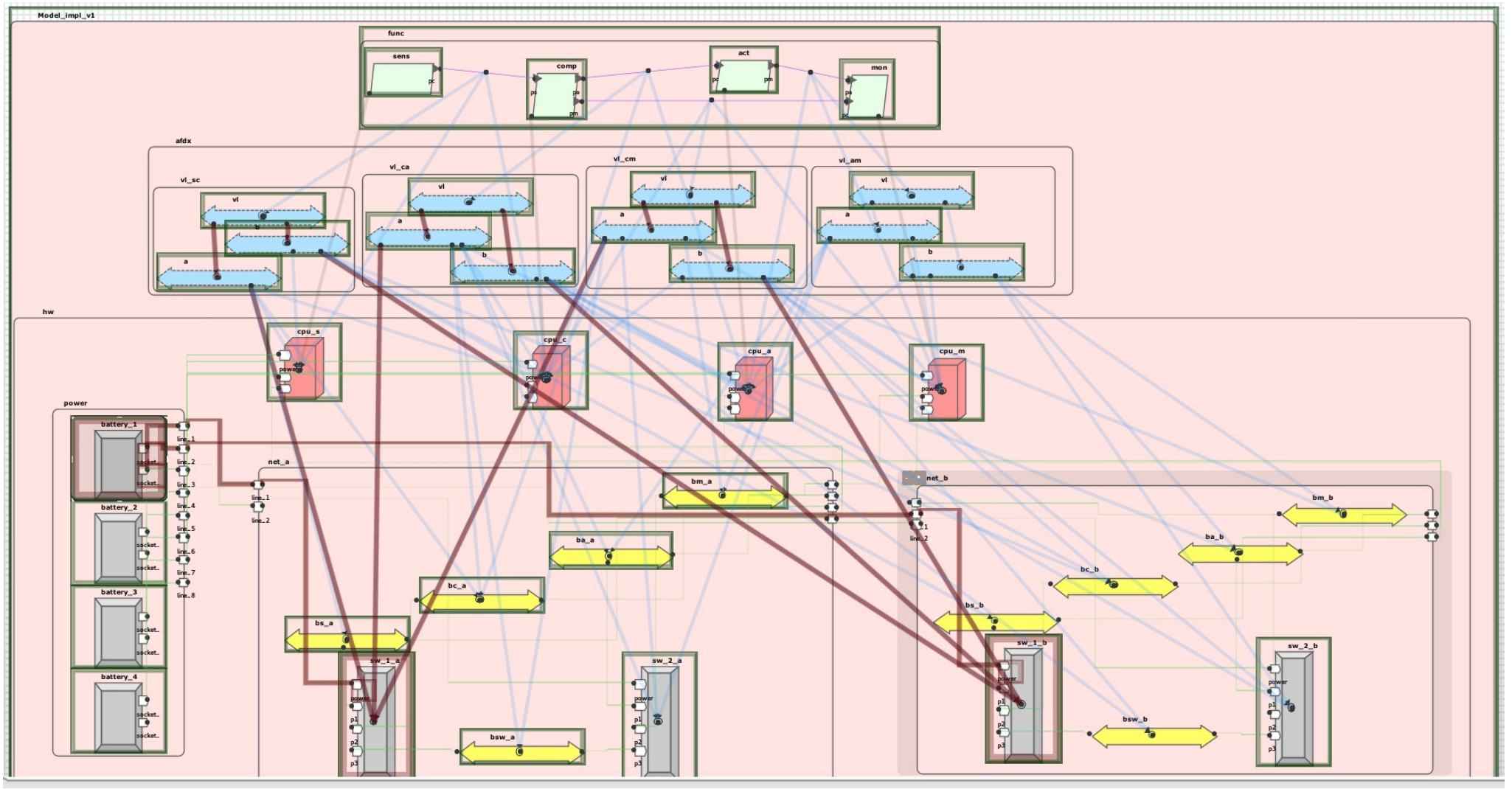
Пример: FMEA


Model_impl_v1
func
sens
comp
act
mon
afdx
vl_sc
vl_ca
vl_cm
vl_am
vl
a
b
hw
cpu_s
cpu_c
cpu_a
cpu_m
power
battery_1
battery_2
battery_3
battery_4
net_a
net_b
bm_a
ba_a
bc_a
bs_a
bsw_a
sw_1_a
sw_2_a
bm_b
ba_b
bc_b
bs_b
bsw_b
sw_1_b
sw_2_b

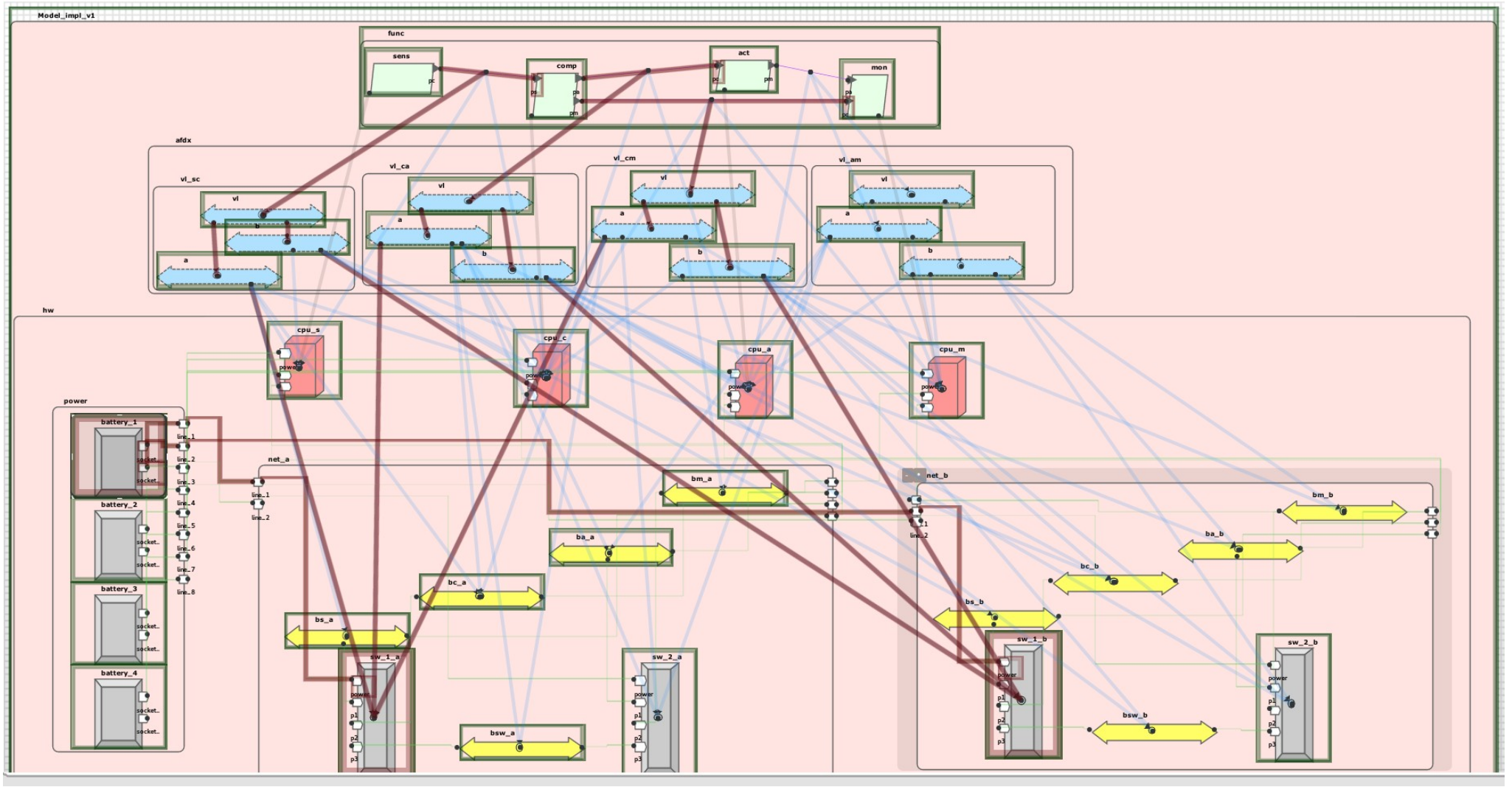
Пример: FMEA


Model_impl_v1
func
sens
comp
act
mon
afdx
vl_sc
vl_ca
vl_cm
vl_am
vl
a
b
hw
cpu_s
cpu_c
cpu_a
cpu_m
power
battery_1
battery_2
battery_3
battery_4
net_a
net_b
bm_a
ba_a
bc_a
bs_a
sw_1_a
sw_2_a
bsw_a
bm_b
ba_b
bc_b
bs_b
sw_1_b
sw_2_b
bsw_b

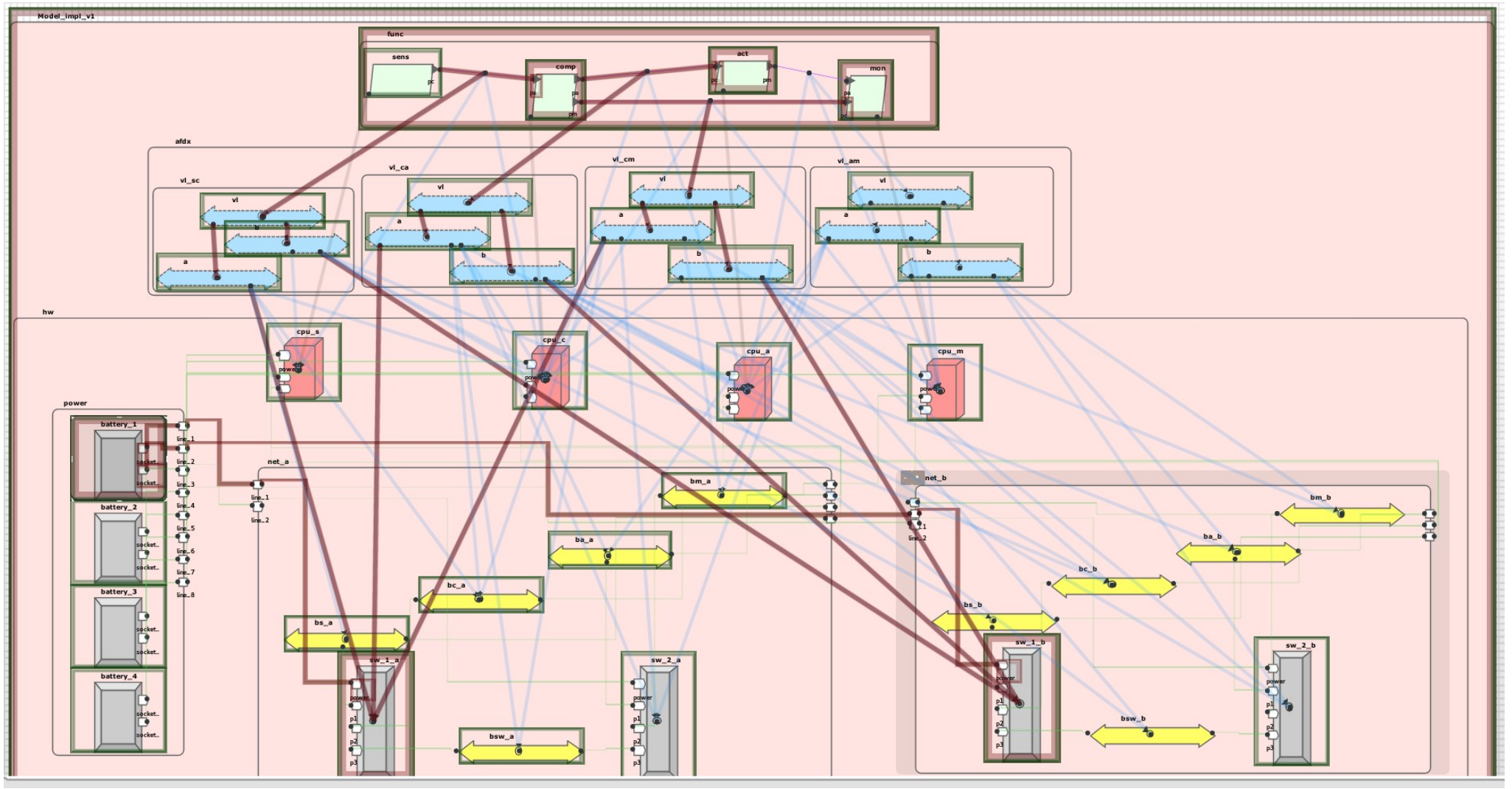
Пример: FMEA


Model_impl_v1
func
sens
comp
act
mon
afdx
vl_sc
vl_ca
vl_cm
vl_am
vl
a
b
hw
cpu_s
cpu_c
cpu_a
cpu_m
power
battery_1
battery_2
battery_3
battery_4
net_a
net_b
bm_a
ba_a
bc_a
bs_a
bsw_a
sw_1_a
sw_2_a
bm_b
ba_b
bc_b
bs_b
bsw_b
sw_1_b
sw_2_b

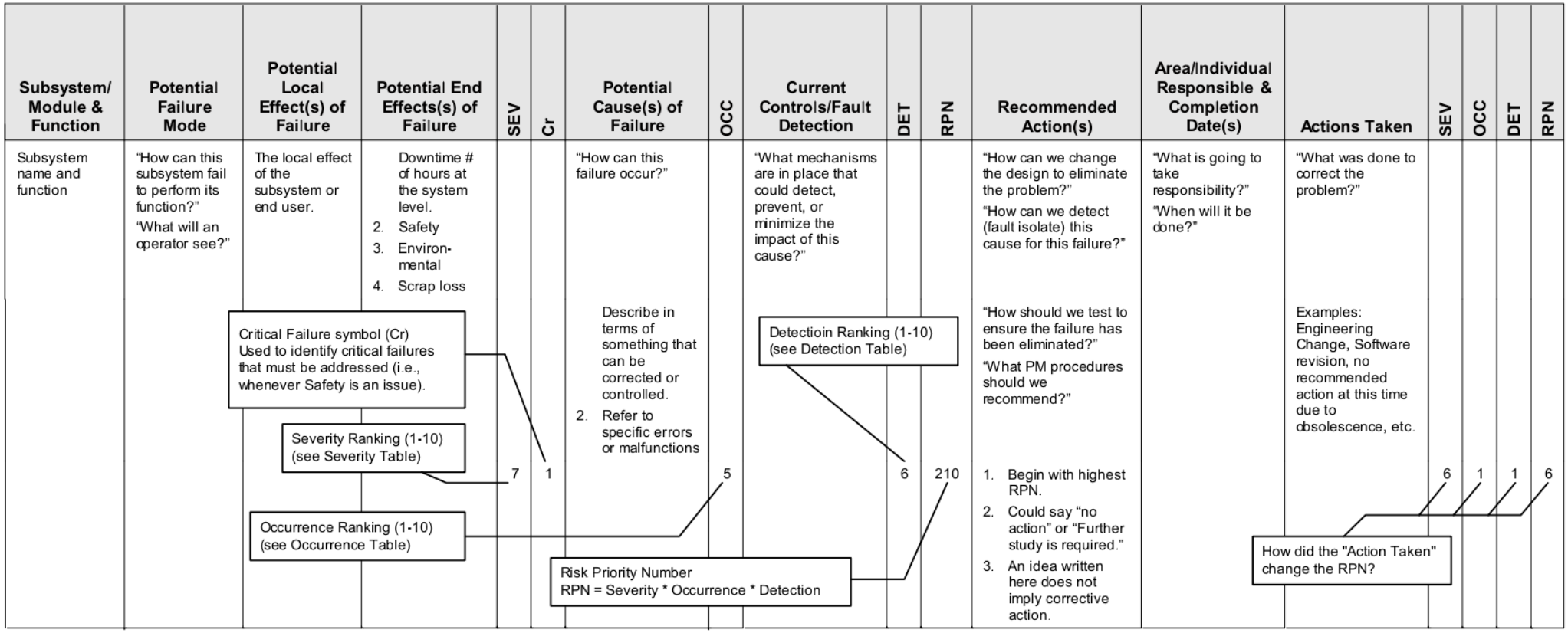
Пример: FMEA


Model_impl_v1
func
sens
comp
act
mon
afdx
vl_sc
vl_ca
vl_cm
vl_am
vl
a
b
hw
cpu_s
cpu_c
cpu_a
cpu_m
power
battery_1
battery_2
battery_3
battery_4
net_a
net_b
bm_a
ba_a
bc_a
bs_a
sw_1_a
sw_2_a
bsw_a
bm_b
ba_b
bc_b
bs_b
sw_1_b
sw_2_b
bsw_b

Пример: последствия отказа



FMEA: рабочая таблица



Проблемы систем

Бурное развитие техники:

- Увеличение количества
- Усложнение
  - Внутреннего строения
  - Внешних связей

=>

- Трудно анализировать
- Требуется автоматизация

Инструмент MASIW

- Modular Avionics System Integrator Workplace
- ИСП РАН + ГосНИИАС
- Моделирование архитектуры
  - AADL
- Моделирование сбоев
  - Error Model Annex
- Автоматический анализ модели
  - Консистентность
  - Симуляция
  - FTA
  - FMEA
  - . . .

AADL:

Architecture Analysis & Design Language

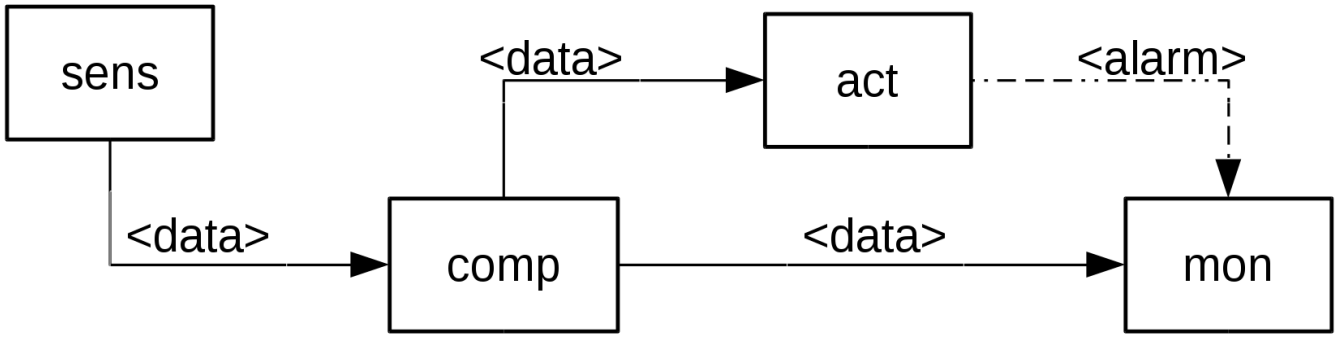
- SAE International standard AS5506C, Architecture Analysis & Design Language (AADL), 2004. Rev. 2017, http://standards.sae.org/as5506c/.
- Ядро + надстройки (annex)
- Текст + графичекое представление
- Переиспользование (package, extend)

AADL: элементы

- Компоненты
  - Type: входы и выходы (черный ящик)
  - Implementation: подкомпоненты (белый ящик)
- Свойства
  - Property: типизированный атрибут
- Взаимодействие
  - Connection: “откуда—куда”
  - Binding: “как / где”

AADL: уровни

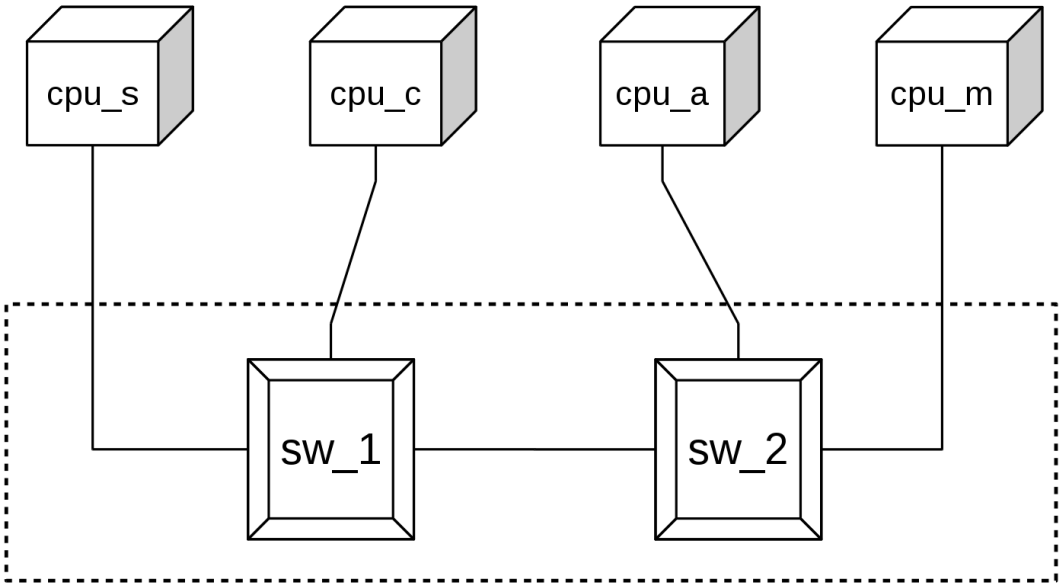
Логический, функциональный



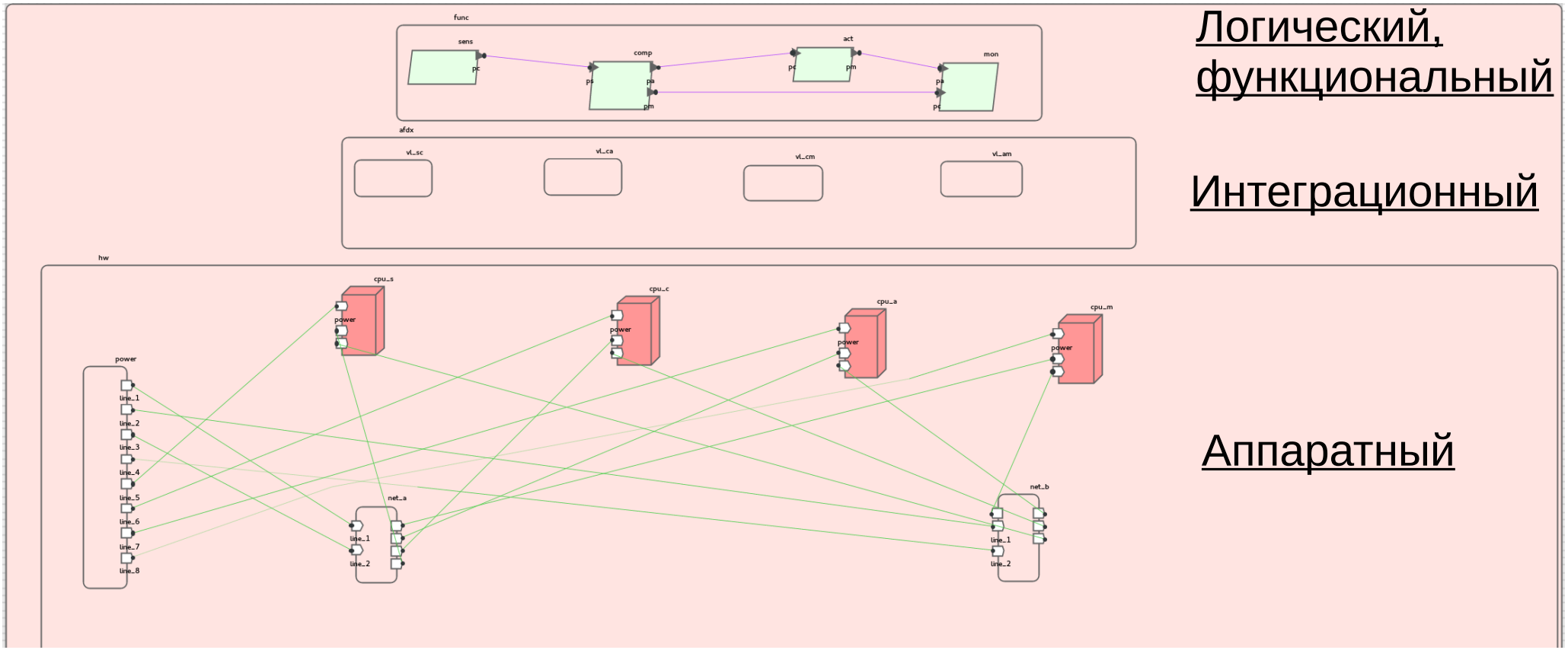
Интеграционный

Протокол AFDX

Аппаратный



Пример

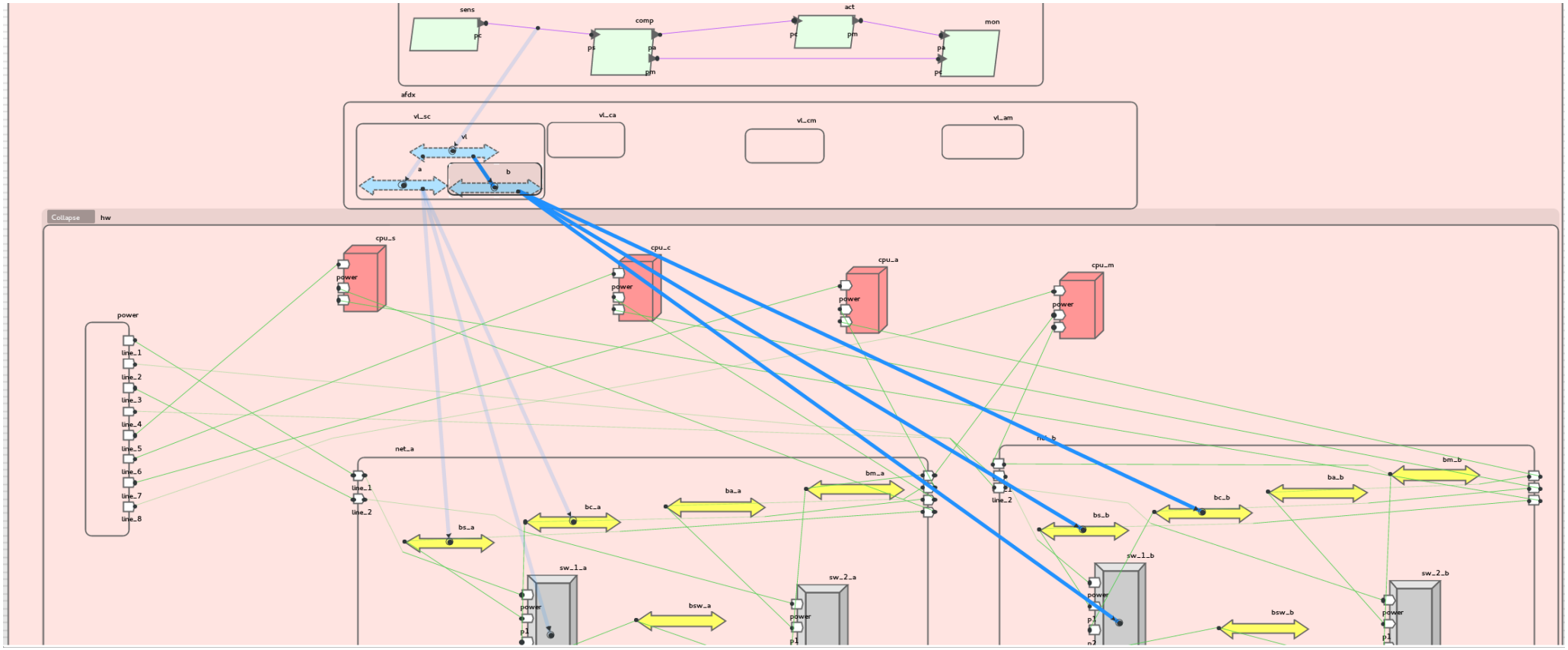


Логический, функциональный

Интеграционный

Аппаратный

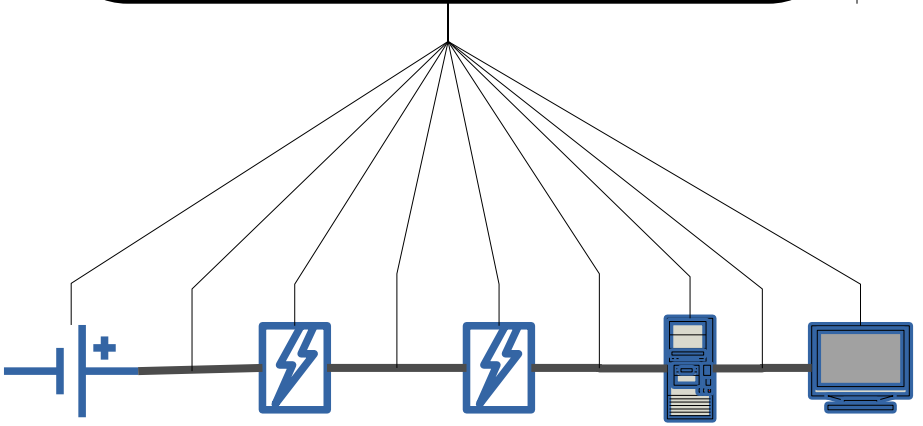
Пример


sens
comp
act
mon
afdx
vl_sc
vl_ca
vl_cm
vl_am
vl
a
b
Collapse
hw
cpu_s
cpu_c
cpu_a
cpu_m
power
line_1
line_2
line_3
line_4
line_5
line_6
line_7
line_8
net_a
net_b
bc_a
ba_a
bm_a
bs_a
bc_b
ba_b
bm_b
bs_b
sw_1_a
sw_2_a
sw_1_b
sw_2_b
bsw_a
bsw_b

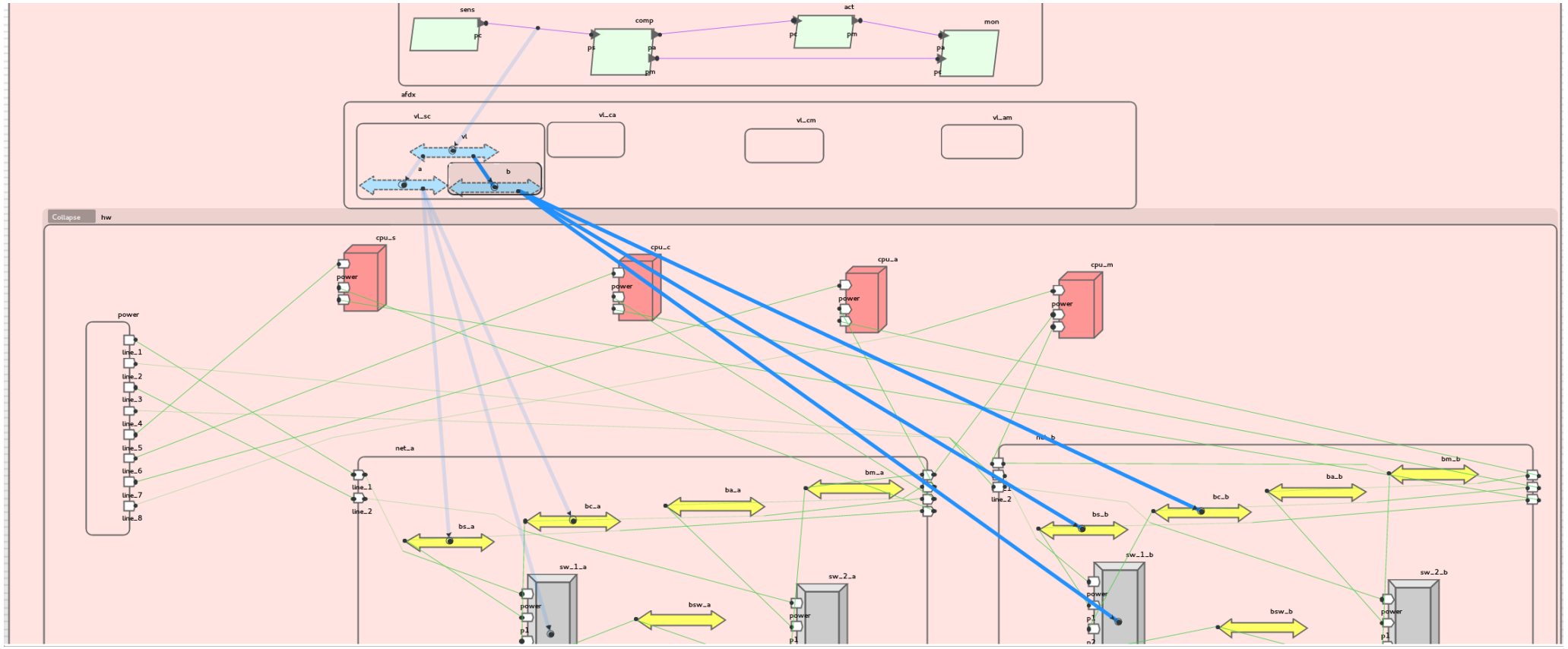
AADL Error Model Annex

- Влияние сбоев в системе
  - Влияние = “причина—следствие”
  - Мгновенное “распространение”
- Средства моделирования:
  - Автомат опасных состояний
  - Влияние (распространение) сбоев
  - Условия переходов
    - Внутренние сбои
    - Наведенные сбои
  - Вероятность/интенсивность сбоев
  - Композиция

```
. . .
transitions
  Op -[ Failure ]-> Failed;
  Op -[ in{NoPower} ]-> Failed;
propagations
   Failed -[]-> out( NoPower );
. . .
```



Распространение ошибок



Пример: вероятности

Компонент	**Сбой**	**Интенсивность**
Коммутатор	Отказ	$2.5 \cdot 10^{-5}$
Процессор	Отказ	$2.5 \cdot 10^{-5}$
Батарея	Отказ	$1.35 \cdot 10^{-5}$

Пример: FMEA

Item(s)	Initial failure mode(s)	End effect	Sev	P
sw_1_a	Отказ	a.[propagation]	9	0.000125
		sw_1_a.Failed	9	0.000125
sw_1_b	Отказ	b.[propagation]	9	0.000125
		sw_1_b.Failed	9	0.000125
battery_1	Отказ	Model. Failed_AppMsg	10	0.0000675

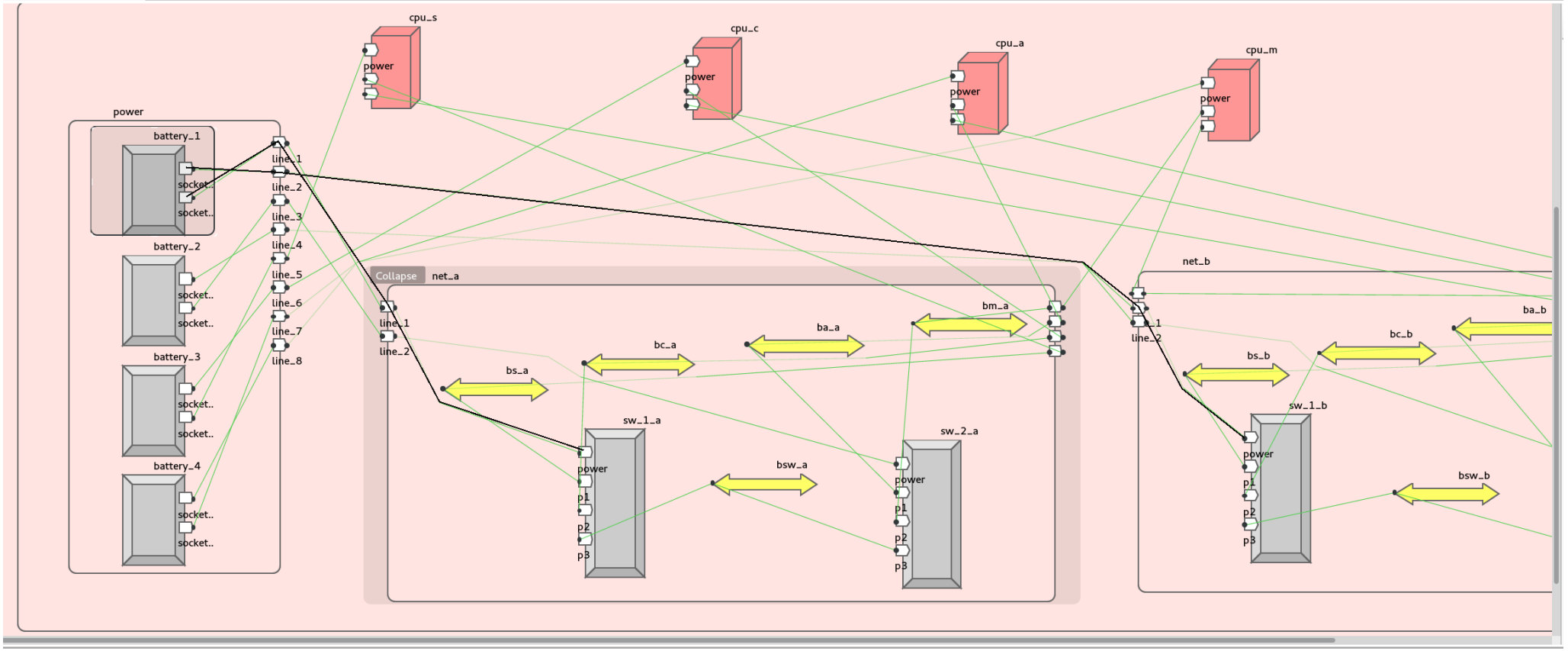
. . .

Пример: проблема

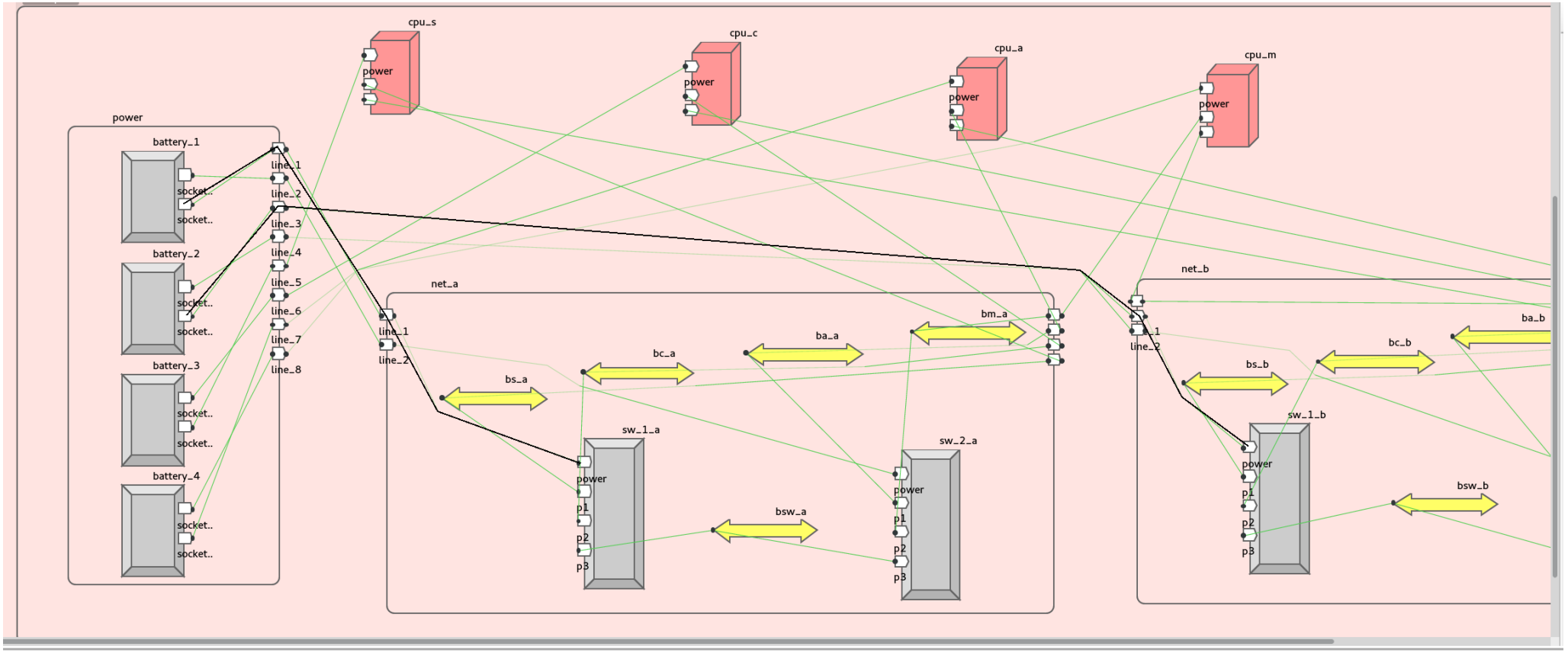
Item(s)	Initial failure mode(s)	End effect	Sev	P
sw_1_a	Отказ	a.[propagation]	9	0.000125
		sw_1_a.Failed	9	0.000125
sw_1_b	Отказ	b.[propagation]	9	0.000125
		sw_1_b.Failed	9	0.000125
battery_1	Отказ	Model. Failed_AppMsg	10	0.0000675

. . .

Пример: причина



Пример: устранение ошибки



Пример: новый FMEA

Item(s)	Initial failure mode(s)	End effect	Sev	P
sw_1_a	Отказ	a.[propagation]	9	0.000125
		sw_1_a.Failed	9	0.000125
sw_1_b	Отказ	b.[propagation]	9	0.000125
		sw_1_b.Failed	9	0.000125
battery_1	Отказ	a.[propagation]	9	0.0000675
		sw_1_a.Failed	9	0.0000675
		sw_2_a.Failed	9	0.0000675
		battery_1.Failed	9	0.0000675
battery_2	Отказ	b.[propagation]	9	0.0000675
		sw_1_b.Failed	9	0.0000675
		sw_2_b.Failed	9	0.0000675
		battery_2.Failed	9	0.0000675

. . .

Результат применения FMEA

- На этапе проектирования системы:
  - Выявить ошибку проектирования
  - Локализовать
  - Устранить

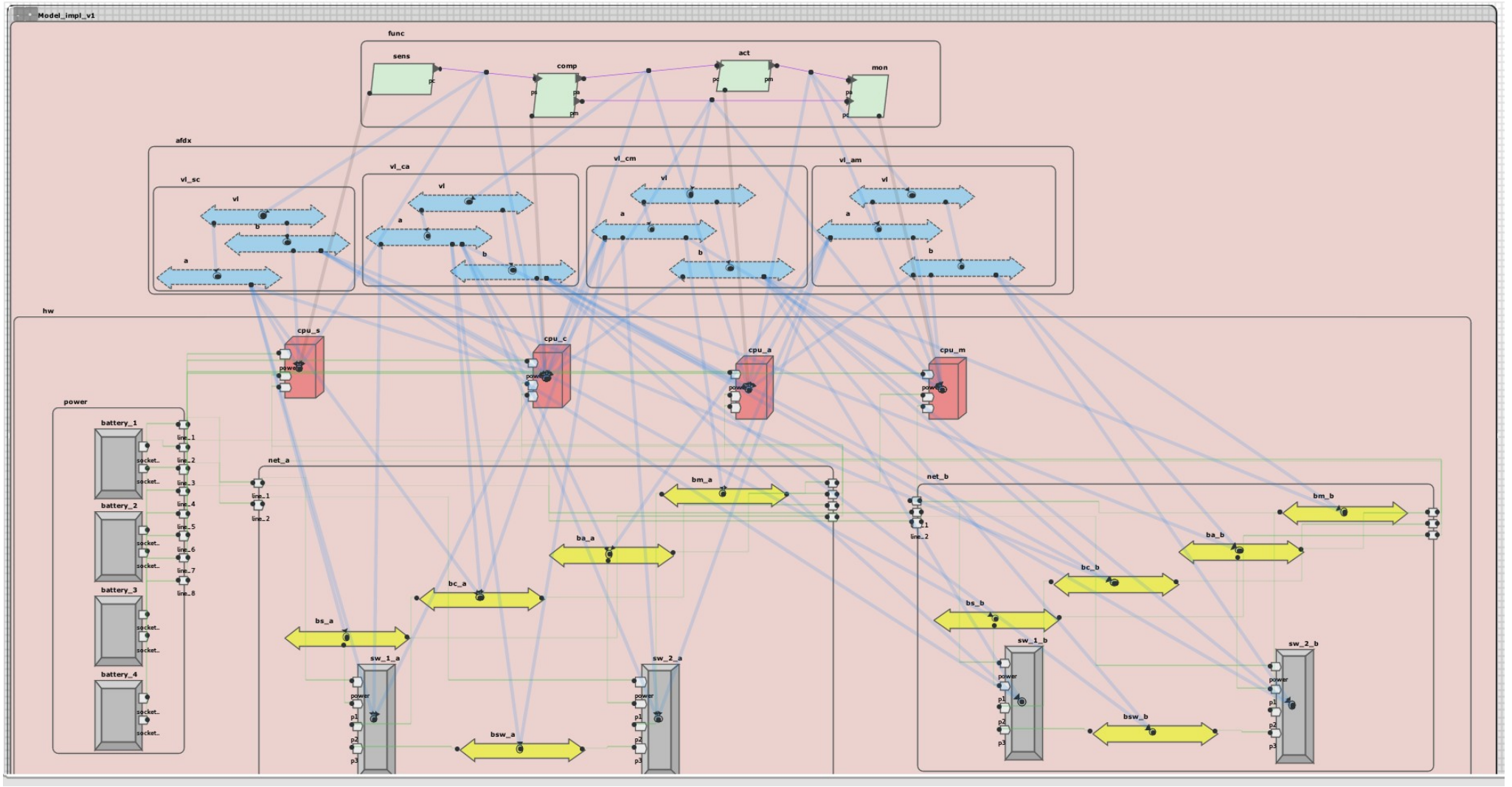
Необходимое условие

- Корректность модели
  - Анализ консистентности
  - “Отладчик”

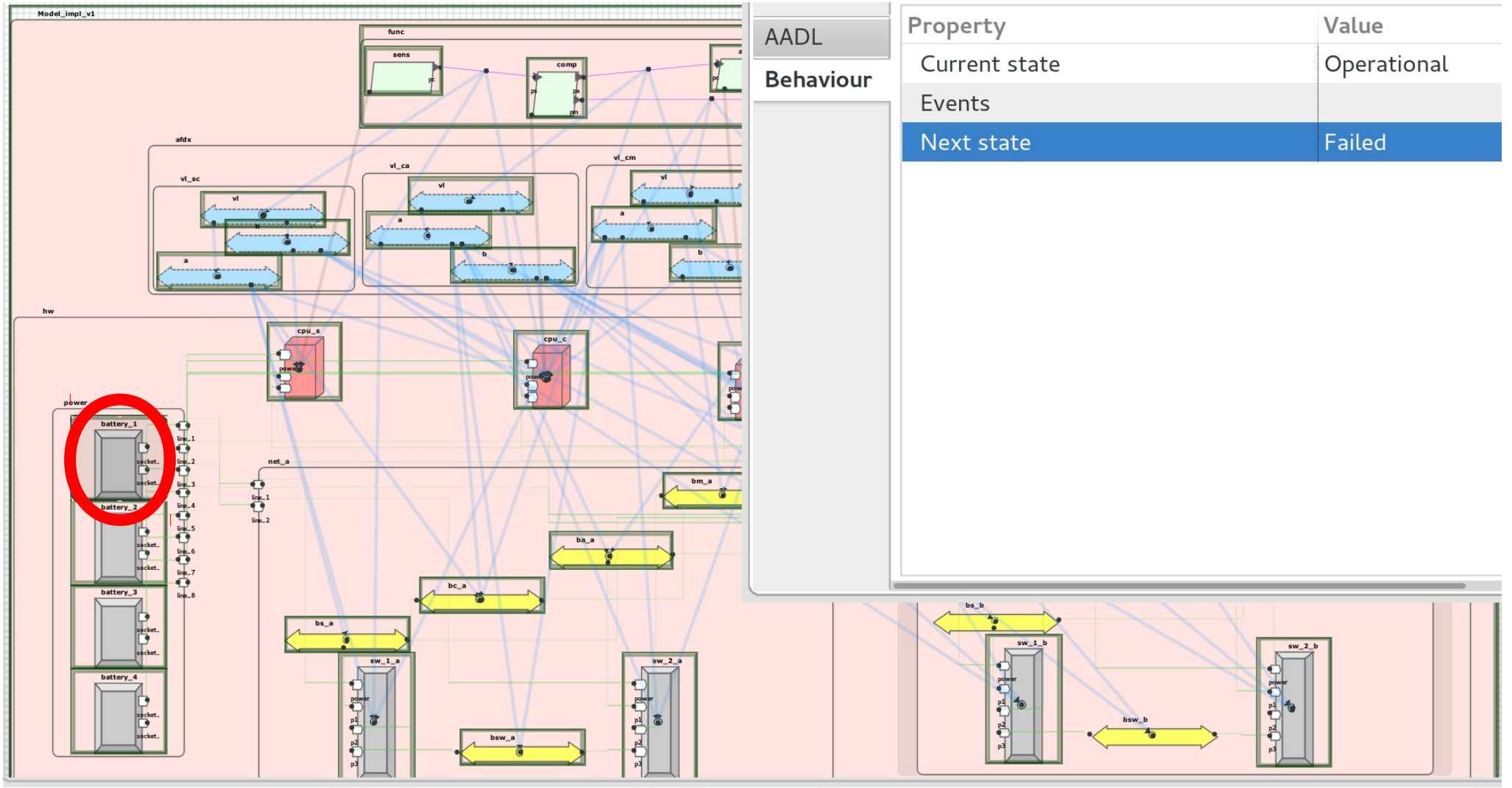
Визуализация FMEA

- Задание исходного состояния
- Запуск анализа
- Мониторинг состояния
- Навигация по истории

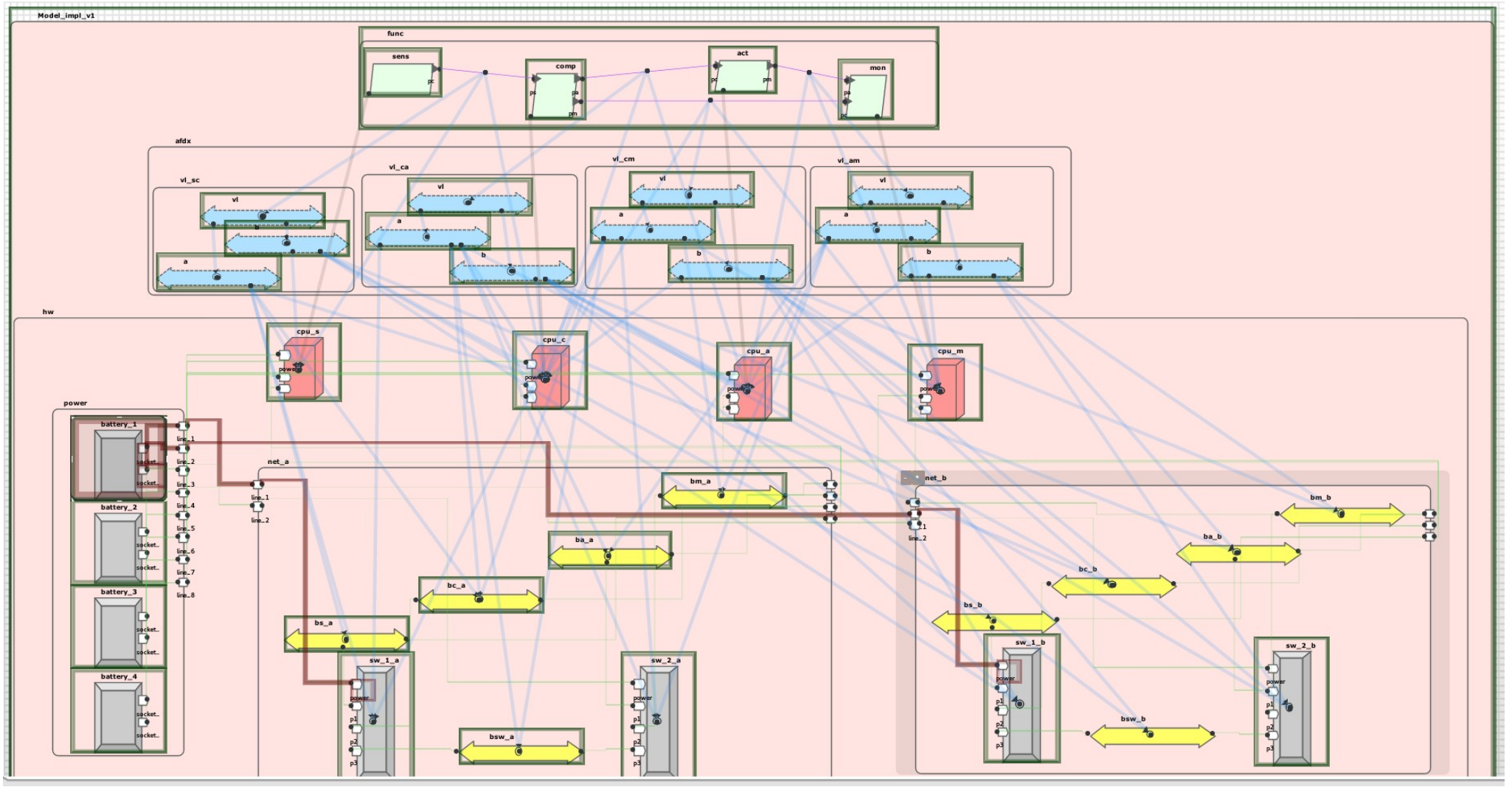
Визуализация FMEA



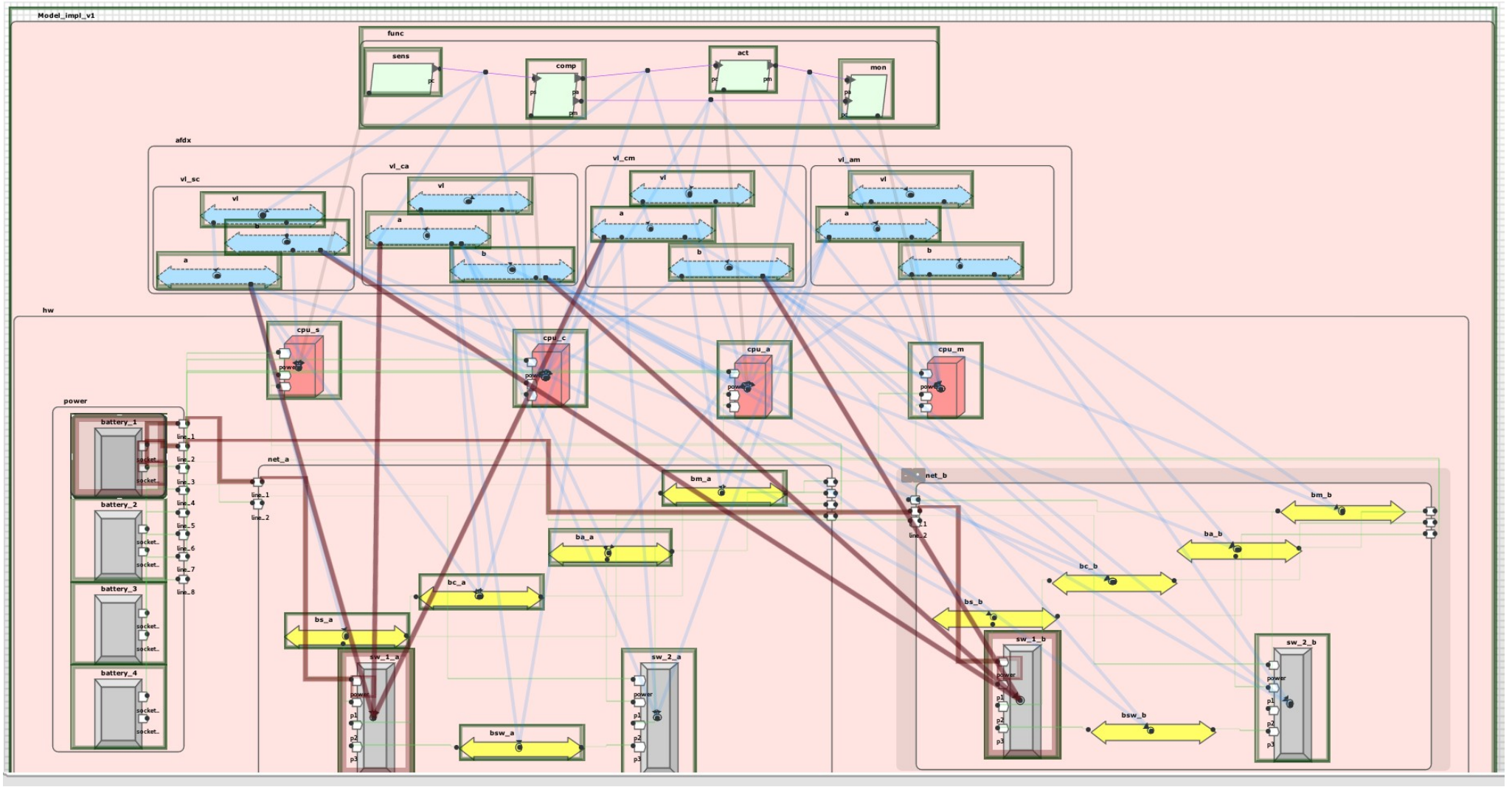
Визуализация FMEA



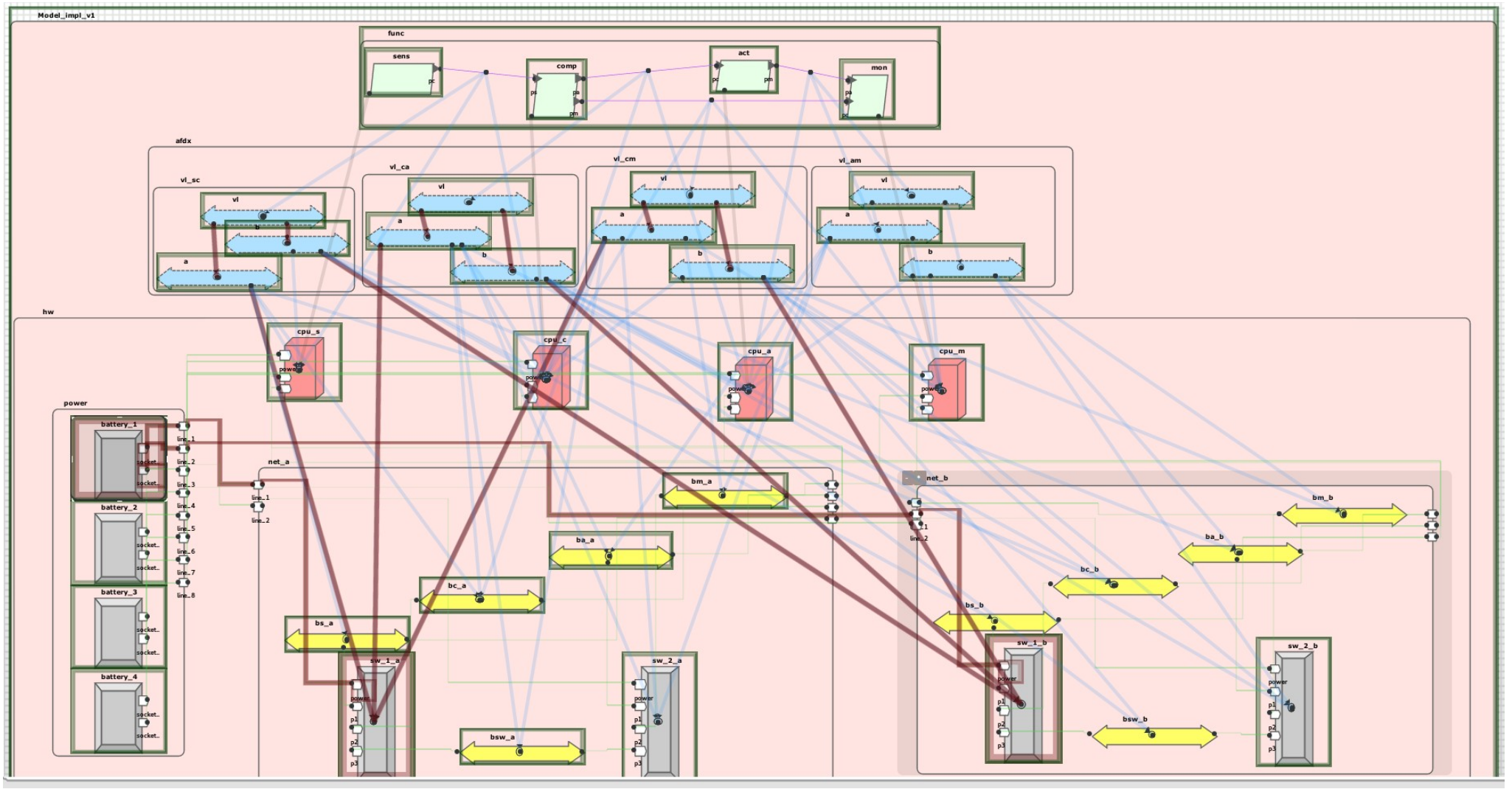
Визуализация FMEA



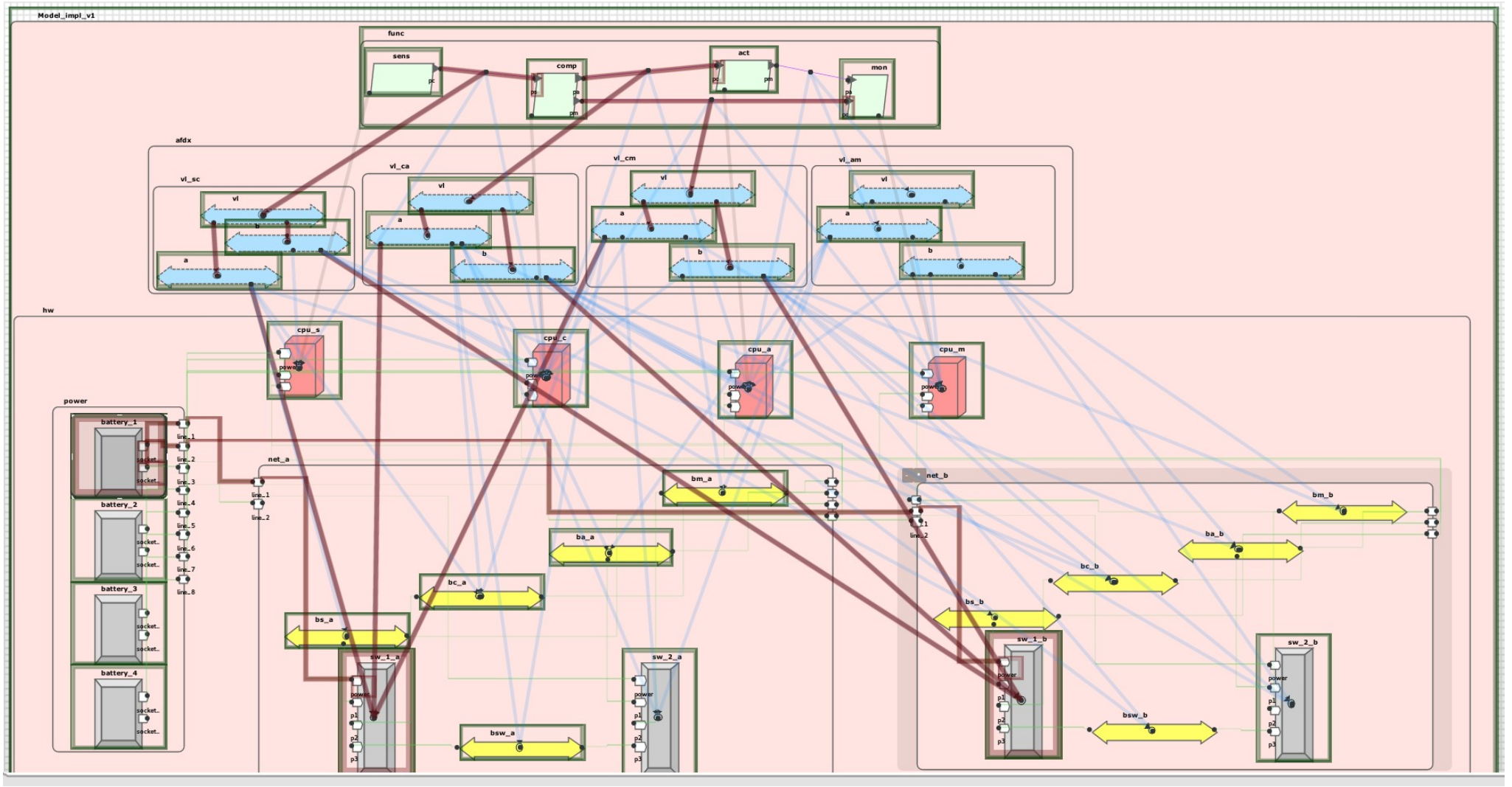
Визуализация FMEA



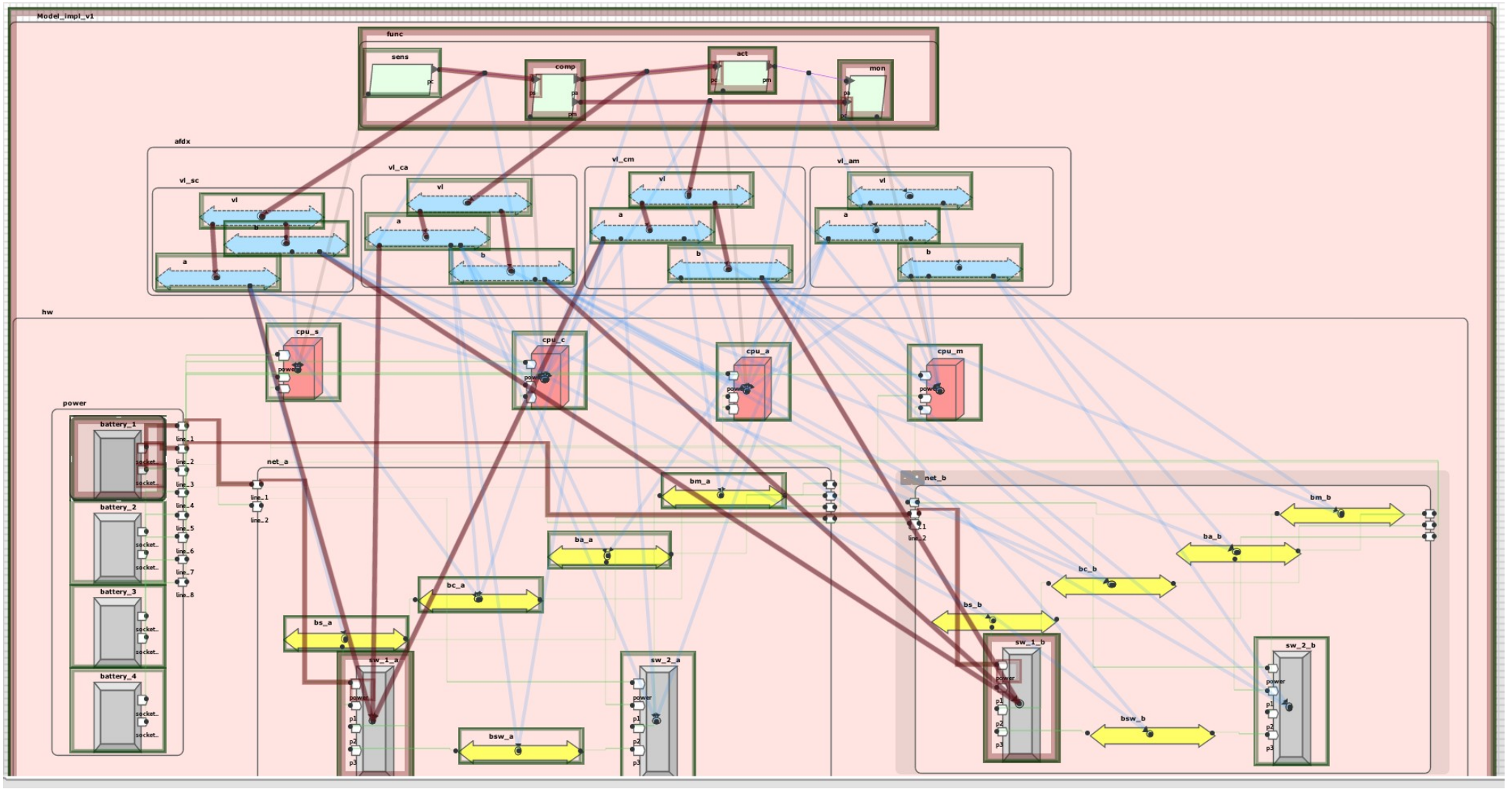
Визуализация FMEA



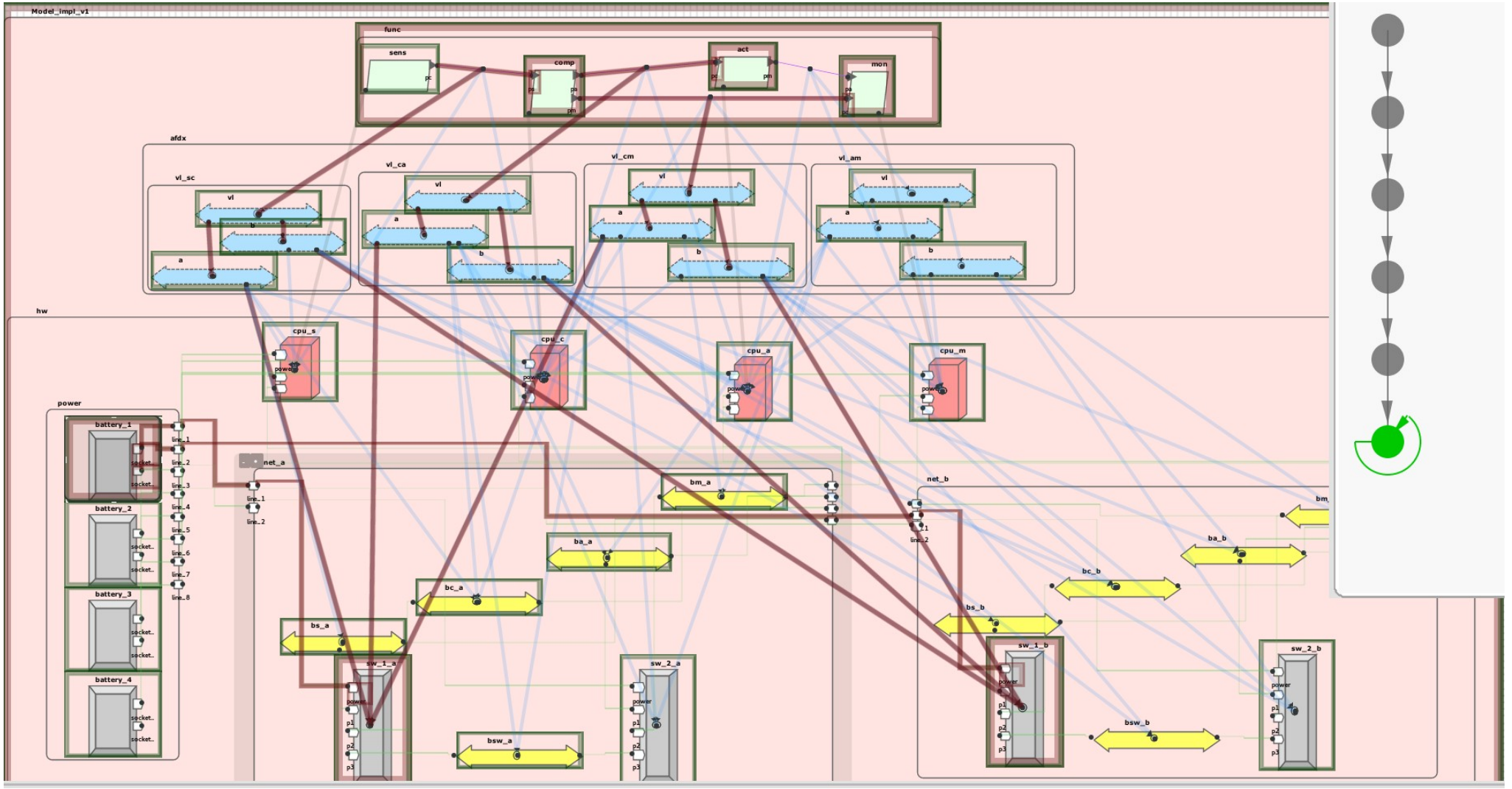
Визуализация FMEA



Визуализация FMEA



Визуализация FMEA



FMEA в MASIW

- Автоматический анализ
  - Для всех компонентов системы
  - Для всех состояний компонентов
  - Для всех сбоев компонентов
- Генерация сводной таблицы
- Визуализация анализа

Спасибо за внимание!