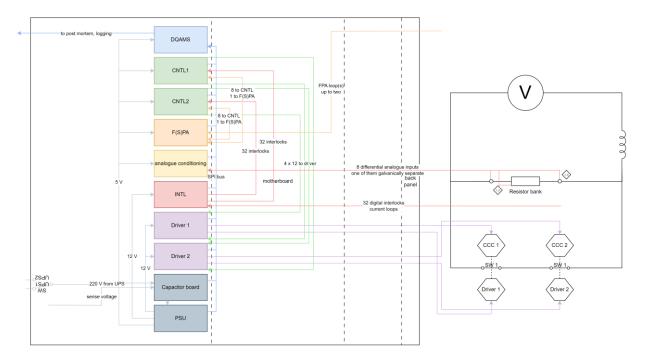
## State of Study

Annotations following meeting



2024 Weekly AFT Meetings, 09/02/2024, Lukas Felsberger

# System Functional Diagram



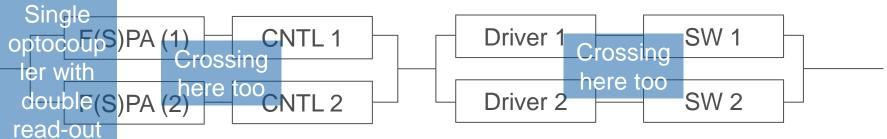


## **Top-Level FMECA**

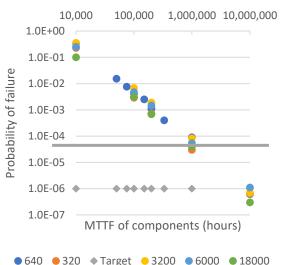
function	failure mode	effect (worst case)	criticality/downtime	reliability target	comment
Interiori			criticality/downtime	reliability target	continent
detect FPA loop open	fail to detect 1 onon cu	witch upon EDA	months	1/100y	
drive switch opening	fail to drive sv		months	1/100y	
	successful ope				
drive switch opening	preventing op	opening	hours	1/y	
collect data and transmit	fail to collect data and transmit (on time)	canno, restart machine until problem diagnosed	hours	1/y	
	•		hours		
continuously drive closed switch		spurious dump	hours	1/y	
collect data and transmit	fail to collect data and transmit (on time)	cannot restart machine until problem diagnosed	hours	1/y	
					there is no active protection of
					the switches by the EE controls i
	fail to datast switches apaping (an time)	DC will trip and cond FDA	hours	14.	case of spurious opening, except vacuum switches
					vacuum switches
- F F		PC will trip and send FPA	nours	1/γ	
•	. ,	cannot restart machine until problem diagnosed	bours	1/v	
			nours	1/9	
detect unsafe operation	fail to detect 2' DIEVAI	nt operation if		1/10v	better discuss on case by case
· · · · · · · · · · · · · · · · · · ·	fail to open sy				better discuss on case by case
open FPA loop		al data at a d		1 1	,
collect data and transmit	fail to collect	ck delected	hours	1/y	
open FPA loop	fail to open FF 2. hoho	viour of pow			
	S. Dena	viour or new			there is no active protection of
		· · · · · · · · · · · · · · · · · · ·			the switches by the EE controls i
		witches under			case of spurious opening, except
open switches	Tail to open sv				vacuum switches
collect data and transmit	fail to collect of	of power	hours	1/y	
	IOSS	or power			
	drive switch opening drive switch opening collect data and transmit detect FPA loop closed continuously drive closed switch collect data and transmit detect switches opening open FPA loop open all other switches collect data and transmit detect unsafe operation open switches open FPA loop collect data and transmit open FPA loop	detect FPA loop open drive switch opening       fail to detect F fail to drive sv successful ope preventing op       1: open sv loop         drive switch opening       preventing op       loop         collect data and transmit       fail to collect data and transmit (on time)         detect FPA loop closed       fail to detect FPA loop closed         continuously drive closed switch       fail to detect FPA loop closed         collect data and transmit       fail to detect FPA loop closed         collect data and transmit       fail to detect switches opening FPA loop)         spuriously open switch (with opening FPA loop)       spuriously open switch (without opening FPA loop)         collect data and transmit       fail to detect switches opening (on time)         open FPA loop       fail to open FPA loop (on time)         open switches       fail to open sv         open switches       fail to open sv         open FPA loop       fail to open FF         collect data and transmit       fail to open FF         collect data and transmit       fail to open sv	detect FPA loop open drive switch opening       fail to detect if fail to drive sv successful ope preventing op collect data and transmit       1: open switch upon FPA loop opening         detect FPA loop closed detect FPA loop closed       fail to detect FPA loop closed       canno restart machine excut problem diagnosed         detect FPA loop closed continuously drive closed switch gene result       fail to detect FPA loop closed       spurious dump spuriously open switch (with opening FPA loop)       spurious dump spurious dump         collect data and transmit       fail to detect switches opening fail to open FPA loop       fail to detect switches opening (on time)       PC will trip and send FPA cannot restart machine until problem diagnosed         detect switches opening open FPA loop open all other switches       fail to detect switches opening (on time)       PC will trip and send FPA PC will trip and send FPA         open FPA loop open switches       fail to detect switches opening (on time)       PC will trip and send FPA         open FPA loop open all other switches       fail to detect if fail to open FPA loop (on time)       PC will trip and send FPA         open FPA loop open switches       fail to detect if fail to open FF       2: prevent operation if interlock detected         open FPA loop       fail to open FF       3: behaviour of new vacuum switches         open FPA loop       fail to open FF       3: behaviour of new vacuum switches         open FPA loop       fail to open sv       5: beha	detect FPA loop open drive switch opening       fail to detect is successful op preventing op       1: open switch upon FPA (oblect data and transmit detect FPA loop closed continuously drive closed switch spuriously open switch (with opening FPA loop) spuriously open switch (with opening FPA loop)       months months months         detect switches opening open FPA loop       fail to detect switches opening fail to open switch (see above)       fail to detect switches opening fail to open FPA loop (on time)       PC will trip and send FPA cannot restart machine until problem diagnosed       hours         detect switches opening open FPA loop       fail to detect switches opening (on time) fail to open switch       PC will trip and send FPA collect data and transmit       hours         detect switches opening open FPA loop       fail to detect switches opening (on time) fail to open sv fail to open	detect FPA loop open fail to detect is fail to detect fPA loop closed fail to collect data and transmit fail to collect data and transmit fon time) detect switches opening open FPA loop fail to collect data and transmit (on time) fail to open FPA loop foil to open FPA loop (on time) open FPA loop fail to collect data and transmit (on time) cannot restart machine until problem diagnosed hours 1/y detect unsafe operation fail to collect data and transmit (on time) cannot restart machine until problem diagnosed hours 1/y detect unsafe operation fail to collect data and transmit (on time) cannot restart machine until problem diagnosed hours 1/y detect unsafe operation fail to collect data and transmit (on time) cannot restart machine until problem diagnosed hours 1/y detect unsafe operation fail to open FPA loop fail to open FPA collect data and transmit fail to collect witches fail to open FPA collect data and transmit fail to collect fail fail to open FPA collect data and transmit fail to open FPA collect data and transmit fail to open FPA collect data and transmit fail to open FPA fail to open FPA



### 1: Simulation of switch opening request



- Simulation model of most critical function generated following last meeting
  - Failure if no path functional and demand (FPA open)
  - Considers that upon each demand, blind failures are discovered and fixed (e.g. if CNTL stopped triggering Driver 1)
- Used to estimate failure rate requirement for the ""boxes"
  - Demand interval varied between 13 and 750 days
  - Based on initial Top-level requirement, failure rate per box ~few hundred FITS (1E6 – 1E7 hours MTTF)
    - FITS: failures in 10<sup>9</sup> hours, example: single discrete components have <10 FITS





### 1: Simulation of switch opening request

Next steps

- Finalize top-level requirements
- Based on requirements, estimate whether boards fulfill
   them based on component prediction
  - To so so, would need design files (processed by design office)
    - SO far: G:\Departments\TE\Projects\EnergyExtraction\UniversalElectronics\GLAB
  - Possibly: FMECA for selected boards to get components on critical path

Id 🔻 Alternate	PN V Description V Category	<ul> <li>PartNumber</li> </ul>	Quantity      CategoryDescription	Page	▼ failure mode ▼ Alph	a V End Effect - User Permit V Comments	v		
1.1 C2	-±10% 50V X7R SMD Multila 217-CA	CC0603_100NF_50V_10%_X7R	1 Capacitor	Critical Permit A	Open	6 False dump		End Effect	▼ Definition ▼
1.1 C2	-±10% 50V X7R SMD Multila 217-CA	CC0603_100NF_50V_10%_X7R	1 Capacitor	Critical Permit A	Parameter change	61 No effect		Blind failure - CIBF	both channels fail
1.1 C2	-±10% 50V X7R SMD Multila 217-CA	CC0603_100NF_50V_10%_X7R	1 Capacitor	Critical Permit A	Short	30 False dump		Blind failure - path	a single channel fa
1.1 C2	-±10% 50V X7R SMD Multila 217-CA	CC0603_100NF_50V_10%_X7R	1 Capacitor	Critical Permit A	Other	3 No effect		False dump	tranmission of a sp
10.1 C3	±10% 50V X7R SMD Multila 217-CA	CC0603_100NF_50V_10%_X7R	1 Capacitor	Test & monitor	Open	6 False dump		Maintenance	allows the current
10.1 C3	-±10% 50V X7R SMD Multila 217-CA	CC0603_100NF_50V_10%_X7R	1 Capacitor	Test & monitor	Parameter change	61 No effect		No effect	having no effect or
10.1.02	-+10% 50V Y7P SMD Multile 217 CA	CC0602 100NIE 50V 10% V7P	1 Capacitor	Tort & monitor	Short	20 Ealco dumo			



## 2: Critical interlocks?

- Document and clarify
  - Discussed e.g. interlock based on dump resistor temperature



3: Behavior of new vacuum switches under loss of power

- Clarify and document
  - New vacuum switches have to be latched not to re-close
  - Clarify and check whether failure rate estimation
     also necessary



# Notes (raw)

- Bozhidar state of EE
  - chassis electronics able to serve all (beyond HL LHC)
    - vacuum, IGBT, FRESCA, Prevessin test station
    - programming of control cards different
    - only connectors different (chassis backpanel)
    - PSU & capacitor boards may still change
    - universal motherboard
    - · backpanel connected to other side of motherboard; connectors adapted to system
- current progress
  - made prototype for vacuum switch (most urgent)
  - launched pre series of ten systems for testing in poland and in charm
  - series design -> little changes by end of sept
    - have tester for PCBs
    - boards are not testable yet
  - launch production Jan/Feb next year
    - go to design office with big order



- our state of study .
  - slide 4: neach FPA channel is actually going to both
    - depending on system different situation •
      - vacuum system
      - focus on vacuum switches
        - needs power upon loss
- next steps .

.

٠

- link to GLAB
- vacuum switch critical path
  - FPA .
  - critical interlock
  - no electricity •
- use a single optocoupler with two outputs ٠
- driver card
  - can be optocoupler (13KA) or relays (600A) •
  - . vacuum sw
    - three operations .
      - . open switch
        - pre charged capacitor
        - done by two fibers
        - same for sw2
        - kill the arc
          - pre charged capactiro
          - after delay activated two fibers
            - . same for sw2
        - trigger CC in opposite direction
          - kill the arc in the other direction
            - (mainly needed for D1 & D2)
        - all done in microseconds
        - keep non vacuum switches with relays in mind
  - other switches .
    - always two relays in series
    - EM switches
      - . cut current - switch opens (slow due to magnetization) - controlled by two relays
      - . transistor to push opening - faster than relay .
      - both fast enough (redundant)
  - bozhidar prepares diagram for vacuum specifically
  - meanwhile we get the full schematics .
  - electricity .
    - UPS 1&2 .
    - distribution box
      - regular circuit breakers
      - . emergency stop
    - transfer switch
      - single line goes to cluster of outlets
    - monitor the output line + line to each vacuum drivers is monitored as well --> fiber to interlock board + 24V transformed -> two PSUs redundant also monitored (four wires)



#### 2024 Weekly AFT Meetings, 09/02/2024, Lukas Felsberger

# Notes (raw)