Reliability studies for a superconducting driver for an ADS linac

Paolo Pierini, Luciano Burgazzi

INFN ENEA

Work supported by the EURATOM 6° framework program of the EC, under contract FI6W-CT-2004-516520

EUROTRANS
- EUROPEAN RESEARCH PROGRAMME FOR THE TRANSMUTATION OF HIGH LEVEL - NUCLEAR WASTE IN AN ACCELERATOR DRIVEN SYSTEM

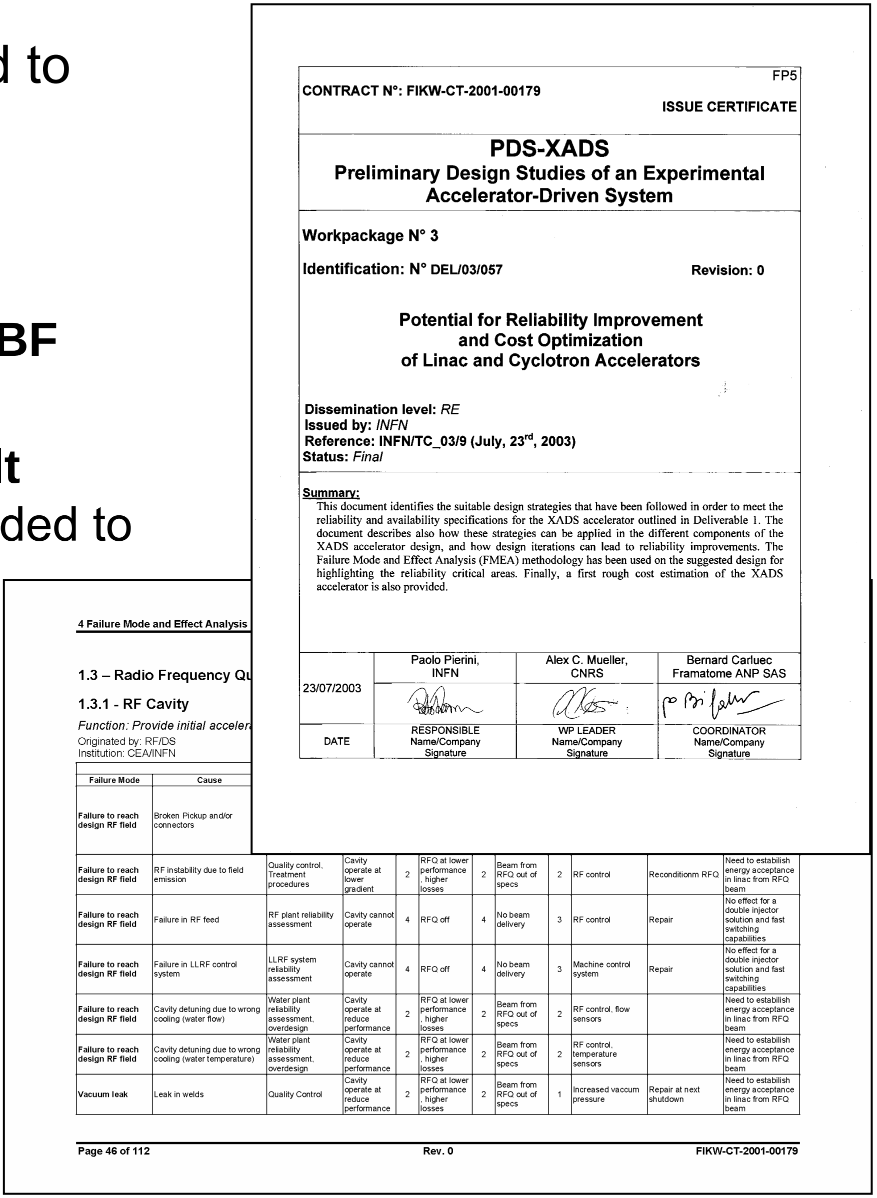
The activity

- Starting with **FP5 PDS-XADS** we have started developing a qualitative FMEA + a lumped-component reliability model of the driver superconducting linac
  - preliminary “parts count” assessment presented at HPPA4

- Extended study to variety of linac configurations
      - » RESS 92 (2007) 449-463
  - concentrate on design issues rather than component data
  - fault tolerance implementation
  - missing of a exhaustive and representative reliability parameter database
- **FP6 EUROTRANS** assumes the same linac layout
- Study extended to show sensitivity to component reliability characteristics

Outcome of FP5 PDS-XADS activities

- Three project deliverables dedicated to reliability assessments
  - Qualitative **FMEA**
  - **RBD** analysis
  - Assessment of (lack of) existing **MTBF** database for components
  - Identification of **redundant and fault tolerant linac configurations** intended to provide nominal reliability characteristics



FP5

CONTRACT N°: FIKW-CT-2001-00179

ISSUE CERTIFICATE

PDS-XADS

Preliminary Design Studies of an Experimental Accelerator-Driven System

Workpackage N° 3

Identification: N° DEL/03/057 **Revision: 0**

Potential for Reliability Improvement and Cost Optimization of Linac and Cyclotron Accelerators

Dissemination level: *RE*
Issued by: *INFN*
Reference: INFN/TC_03/9 (July, 23rd, 2003)
Status: *Final*

Summary:

This document identifies the suitable design strategies that have been followed in order to meet the reliability and availability specifications for the XADS accelerator outlined in Deliverable 1. The document describes also how these strategies can be applied in the different components of the XADS accelerator design, and how design iterations can lead to reliability improvements. The Failure Mode and Effect Analysis (FMEA) methodology has been used on the suggested design for highlighting the reliability critical areas. Finally, a first rough cost estimation of the XADS accelerator is also provided.

23/07/2003	Paolo Pierini, INFN	Alex C. Mueller, CNRS	Bernard Carluec Framatome ANP SAS
DATE	RESPONSIBLE Name/Company Signature	WP LEADER Name/Company Signature	COORDINATOR Name/Company Signature

4 Failure Mode and Effect Analysis

1.3 – Radio Frequency Qu

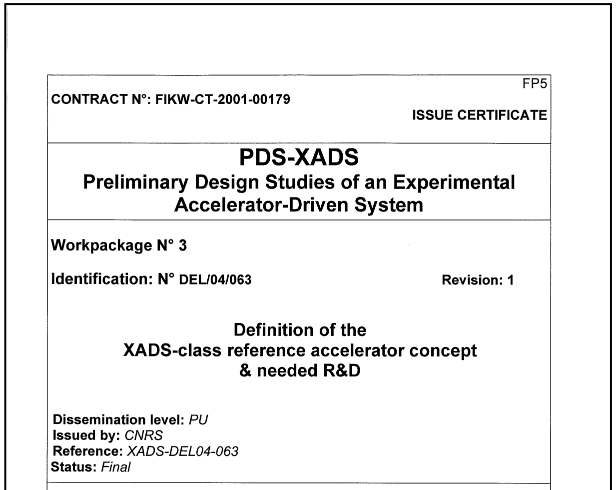
1.3.1 - RF Cavity

Function: Provide initial acceler

Originated by: RF/DS
Institution: CEA/INFN

Failure Mode	Cause										
Failure to reach design RF field	Broken Pickup and/or connectors										
Failure to reach design RF field	RF instability due to field emission	Quality control, Treatment procedures	Cavity operate at lower gradient	2	RFQ at lower performance , higher losses	2	Beam from RFQ out of specs	2	RF control	Reconditionm RFQ	Need to estabilish energy acceptance in linac from RFQ beam
Failure to reach design RF field	Failure in RF feed	RF plant reliability assessment	Cavity cannot operate	4	RFQ off	4	No beam delivery	3	RF control	Repair	No effect for a double injector solution and fast switching capabilities
Failure to reach design RF field	Failure in LLRF control system	LLRF system reliability assessment	Cavity cannot operate	4	RFQ off	4	No beam delivery	3	Machine control system	Repair	No effect for a double injector solution and fast switching capabilities
Failure to reach design RF field	Cavity detuning due to wrong cooling (water flow)	Water plant reliability assessment, overdesign	Cavity operate at reduce performance	2	RFQ at lower performance , higher losses	2	Beam from RFQ out of specs	2	RF control, flow sensors		Need to estabilish energy acceptance in linac from RFQ beam
Failure to reach design RF field	Cavity detuning due to wrong cooling (water temperature)	Water plant reliability assessment, overdesign	Cavity operate at reduce performance	2	RFQ at lower performance , higher losses	2	Beam from RFQ out of specs	2	RF control, temperature sensors		Need to estabilish energy acceptance in linac from RFQ beam
Vacuum leak	Leak in welds	Quality Control	Cavity operate at reduce performance	2	RFQ at lower performance , higher losses	2	Beam from RFQ out of specs	1	Increased vaccum pressure	Repair at next shutdown	Need to estabilish energy acceptance in linac from RFQ beam

Page 46 of 112 **Rev. 0** **FIKW-CT-2001-00179**



FP5

CONTRACT N°: FIKW-CT-2001-00179

ISSUE CERTIFICATE

PDS-XADS

Preliminary Design Studies of an Experimental Accelerator-Driven System

Workpackage N° 3

Identification: N° DEL/04/063 **Revision: 1**

Definition of the XADS-class reference accelerator concept & needed R&D

Dissemination level: *PU*
Issued by: *CNRS*
Reference: *XADS-DEL04-063*
Status: *Final*

Definition of the reliability objectives

- Define a **Mission Time**, the operation period for which we need to carry out estimations
  - Depends on design of subcritical assembly/fuel cycle
- Define **parameter** for reliability goal
  - Fault Rate, i.e. Number of system faults per mission
  - Availability
  - No concern on R parameter at mission time
    - R is the survival probability
    - relevant for mission critical (non repairable environments)
- Provide **corrective maintenance** “rules” on elements
  - Components in the accelerator tunnel can be repaired only during system halt
    - Personnel protection issues in radiation areas
  - Redundant components in shielded areas can be repaired immediately

Reliability goal

- Assumed XT-ADS
  - 3 months of continuous operation with < 3 trips per period
  - 1 month of long shutdown
  - 3 operation cycles per year
  - 10 trips per year

  - no constraints on R

Mission Time	2190 hours
Goal MTBF	~ 700 hours
Goal number of failures per mission	~ 3
Reliability parameter	Unconstrained

RAMS

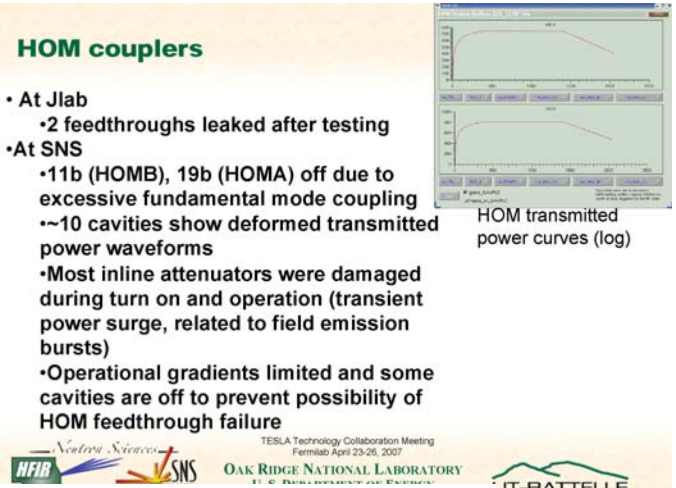
- Baseline idea: use a commercial available RAMS tool for formal accelerator reliability estimations
  - Powerful RBD analysis
  - Montecarlo evalutation
  - Elaborated connection configurations
    - Hot parallelism
    - Standby parallelism
    - Warm parallelism
    - “k/n” parallelism
  - Many options for maintenance schemes and actions (both preventive & corrective, “kludge fixes”, etc.)
    - Eg: fix when system fails or fix when component fail (it’s the same only for series connection)
    - can easily account for maintenance cost and repair and spare logistics
  - Not used at all in accelerator community

What kind of faults are in component MTBF?

- MTBF is used for random failure events
- Every failure that is highly predictable should get out of the MTBF estimations, and goes into the (preemptive) maintenance analysis
  - eg. Components wear out, failures related to bad design, Aging (if we perform a constant failure rate analysis)
- Example: CRT Monitor in a RBD block
  - MTBF of 100.000 h
  - But we know that CRT phosphors do not last 11 years! Monitors need to be changed after 5.000 h of operations or so.
  - The “bath-tub” curve…
- **Trivial concepts within communities where reliability standards have been applied since decades**
  - Not so clear in accelerator community, hence confusing DB

Design issues

- Often many “reliability” problems can be truly identified as component design issues (weak design) or improper operation (above rated values)
- e.g. very successful SNS operation
  - problems due to components providing non critical functionalities but with failure modes with drastic consequences



HOM couplers

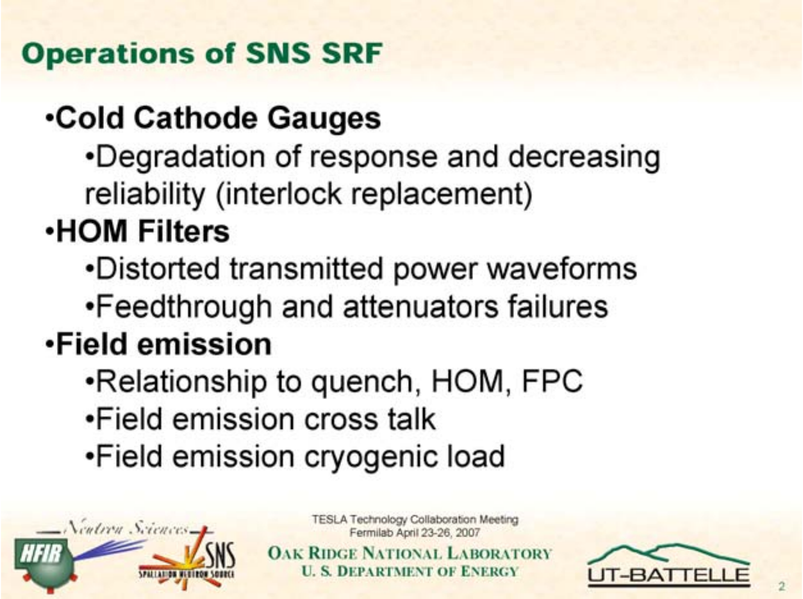
- At Jlab
  - 2 feedthroughs leaked after testing
- At SNS
  - 11b (HOMB), 19b (HOMA) off due to excessive fundamental mode coupling
  - ~10 cavities show deformed transmitted power waveforms
  - Most inline attenuators were damaged during turn on and operation (transient power surge, related to field emission bursts)
  - Operational gradients limited and some cavities are off to prevent possibility of HOM feedthrough failure

HOM transmitted power curves (log)

TESLA Technology Collaboration Meeting
Fermilab April 23-26, 2007

Oak Ridge National Laboratory

8



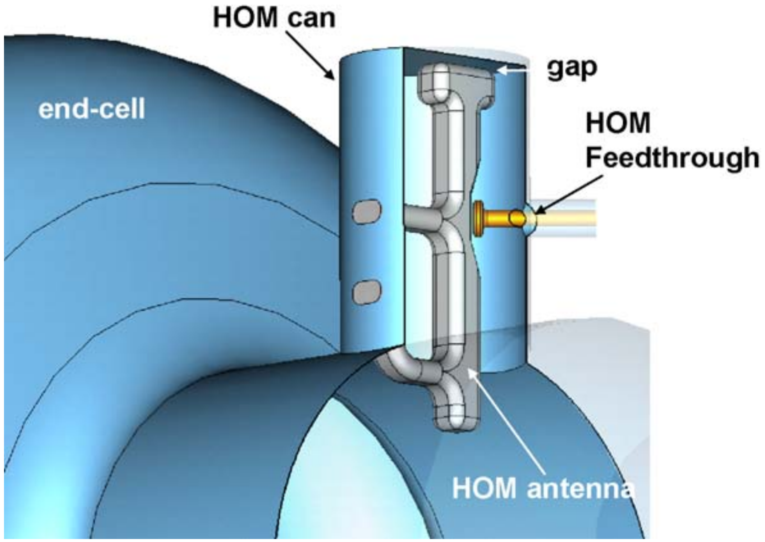
Operations of SNS SRF

- Cold Cathode Gauges
  - Degradation of response and decreasing reliability (interlock replacement)
- HOM Filters
  - Distorted transmitted power waveforms
  - Feedthrough and attenuators failures
- Field emission
  - Relationship to quench, HOM, FPC
  - Field emission cross talk
  - Field emission cryogenic load

TESLA Technology Collaboration Meeting
Fermilab April 23-26, 2007

Oak Ridge National Laboratory
U. S. Department of Energy

2



CHL event

- On February 25th a loss of communication between an IOC and a PLC in the CHL resulted in over pressurization of the He return header and of all the cavities to 2.2 atm.
- Negative impact: three tuners were damaged (being repaired as we speak)
- Positive impact: the system was pressure tested a significant fraction of the pressure vessel code requirements

LHC

Fermilab Today

Tuesday, April 3, 2007

Subscribe | Contact *Fermilab Today* | Archive | Classifieds

Search GO

Fermilab Update on Inner Triplet Magnets at LHC

On Tuesday, March 27, a Fermilab-built quadrupole magnet, one of an "inner triplet" of three focusing magnets, failed a high-pressure test at Point 5 in the tunnel of the LHC accelerator at CERN. Since Tuesday, teams at CERN and Fermilab have worked closely together to address the problem and have identified the cause of the failure. Now they are at work on a solution.

The asymmetric force generated by the pressure of the test broke the supports in magnet Q1 that hold the magnet's cold mass inside the cryostat, which also resulted in damage to the electrical connections. The status of the Q1 cold mass itself is still being determined, as is the status of the other two magnets in the triplet, Q2 and Q3. Also under investigation is the status of a distribution feed box, or DFBX, designed to provide cryogenic fluids and electrical power for the inner triplet magnets.

The magnet supports are made of a material called G-11, a glass cloth-epoxy laminate. The specifications for the magnet designate 20 atmospheres as the design pressure criterion and 25 atmospheres as the acceptance test criterion. However, computer-aided engineering calculations completed independently by Fermilab and CERN on March 28 show that the G-11 support structure in the magnets was inadequate to withstand the associated longitudinal forces. CERN and Fermilab now know that this is an intrinsic design flaw that must be addressed in all triplet magnets assembled at Fermilab.

Review of engineering design documentation reveals that the longitudinal force generated by asymmetric loading was not included in the engineering design or identified as an issue in the four design reviews that were carried out.

Q1 Quadrupole Magnet – CERN and Fermilab are working to identify repairs to the structures that hold the cold mass (blue) in place within the cryostat (orange) in each magnet of the triplet on either side of the LHC's four interaction points. The Q1 magnet of each triplet is the magnet closest to the interaction point (IP).

Longitudinal force during a pressure test broke the G-11 support structure (green) securing the cold mass (blue) inside the magnet cryostat (not shown).

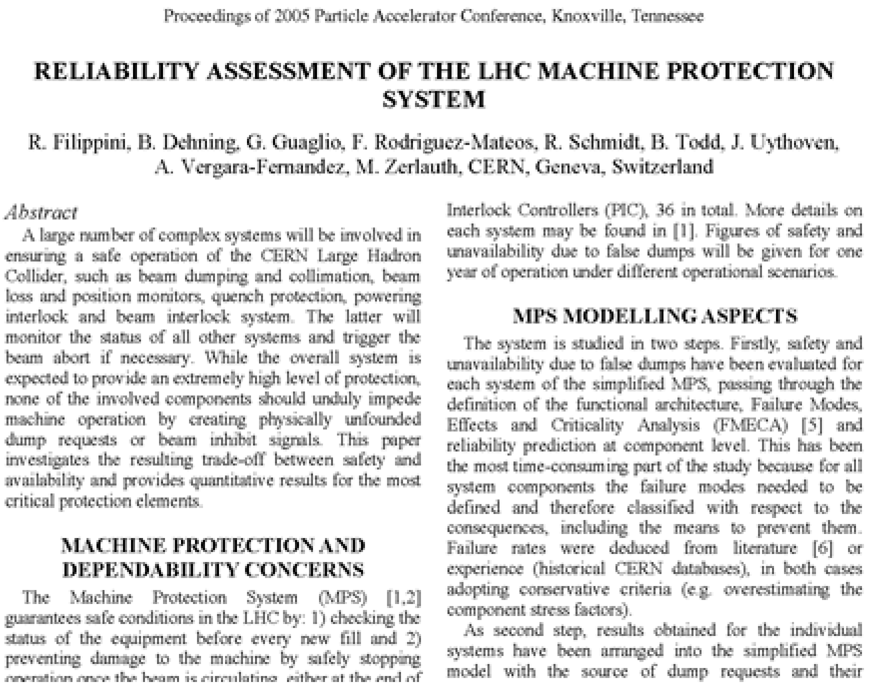
Also **design reviews** and **risk analysis procedures** are different in the 2 communities

March 2007 LHC magnet failure in tunnel

a foreseen test condition was not in the design specs

But also cases of significant design effort

- LHC Machine Protection system
  - Energy stored in each of the 2 proton beams will be 360 MJ
  - If lost without control serious damage to hardware
    - 1 kg of copper melts with 700 kJ
  - Analysis meant to trade off safety (probability of undetected beam losses leading to machine damage) and availability (number of false beam trips per year induced by the system)
  - Complete reliability modeling
- LHC magnets Quench Protection System
  - Huge energy stored in SC magnets (10 GJ)
  - Needs to be gracefully handled



Proceedings of 2005 Particle Accelerator Conference, Knoxville, Tennessee

RELIABILITY ASSESSMENT OF THE LHC MACHINE PROTECTION SYSTEM

R. Filippini, B. Dehning, G. Guaglio, F. Rodriguez-Mateos, R. Schmidt, B. Todd, J. Uythoven,
A. Vergara-Fernandez, M. Zerlauth, CERN, Geneva, Switzerland

Abstract

A large number of complex systems will be involved in ensuring a safe operation of the CERN Large Hadron Collider, such as beam dumping and collimation, beam loss and position monitors, quench protection, powering interlock and beam interlock system. The latter will monitor the status of all other systems and trigger the beam abort if necessary. While the overall system is expected to provide an extremely high level of protection, none of the involved components should unduly impede machine operation by creating physically unfounded dump requests or beam inhibit signals. This paper investigates the resulting trade-off between safety and availability and provides quantitative results for the most critical protection elements.

MACHINE PROTECTION AND DEPENDABILITY CONCERNS

The Machine Protection System (MPS) [1,2] guarantees safe conditions in the LHC by: 1) checking the status of the equipment before every new fill and 2) preventing damage to the machine by safely stopping operation once the beam is circulating, either at the end of

Interlock Controllers (PIC), 36 in total. More details on each system may be found in [1]. Figures of safety and unavailability due to false dumps will be given for one year of operation under different operational scenarios.

MPS MODELLING ASPECTS

The system is studied in two steps. Firstly, safety and unavailability due to false dumps have been evaluated for each system of the simplified MPS, passing through the definition of the functional architecture, Failure Modes, Effects and Criticality Analysis (FMECA) [5] and reliability prediction at component level. This has been the most time-consuming part of the study because for all system components the failure modes needed to be defined and therefore classified with respect to the consequences, including the means to prevent them. Failure rates were deduced from literature [6] or experience (historical CERN databases), in both cases adopting conservative criteria (e.g. overestimating the component stress factors).

As second step, results obtained for the individual systems have been arranged into the simplified MPS model with the source of dump requests and their

Lumped components database

- Reduce the accelerator complexity to a simple system
- System composed of “lumped” components
  - Various sources: IFMIF, SNS, APT estimates, internal eng. judg.
  - + a bit of optimism and realism

System	Subsystem	MTBF (h)	MTTR (h)
Injector	Proton Source	1,000	2
	RFQ	1,200	4
	NC DTL	1,000	2
Support Systems	Cryoplant	3,000	10
	Cooling System	3,000	2
	Control System	3,000	2
RF Unit	High Voltage PS	30,000	4
	Low Level RF	100,000	4
	Transmitters	10,000	4
	Amplifier	50,000	4
	Power Components	100,000	12
Beam Delivery System	Magnets	1,000,000	1
	Power Supplies	100,000	1

MTBF data

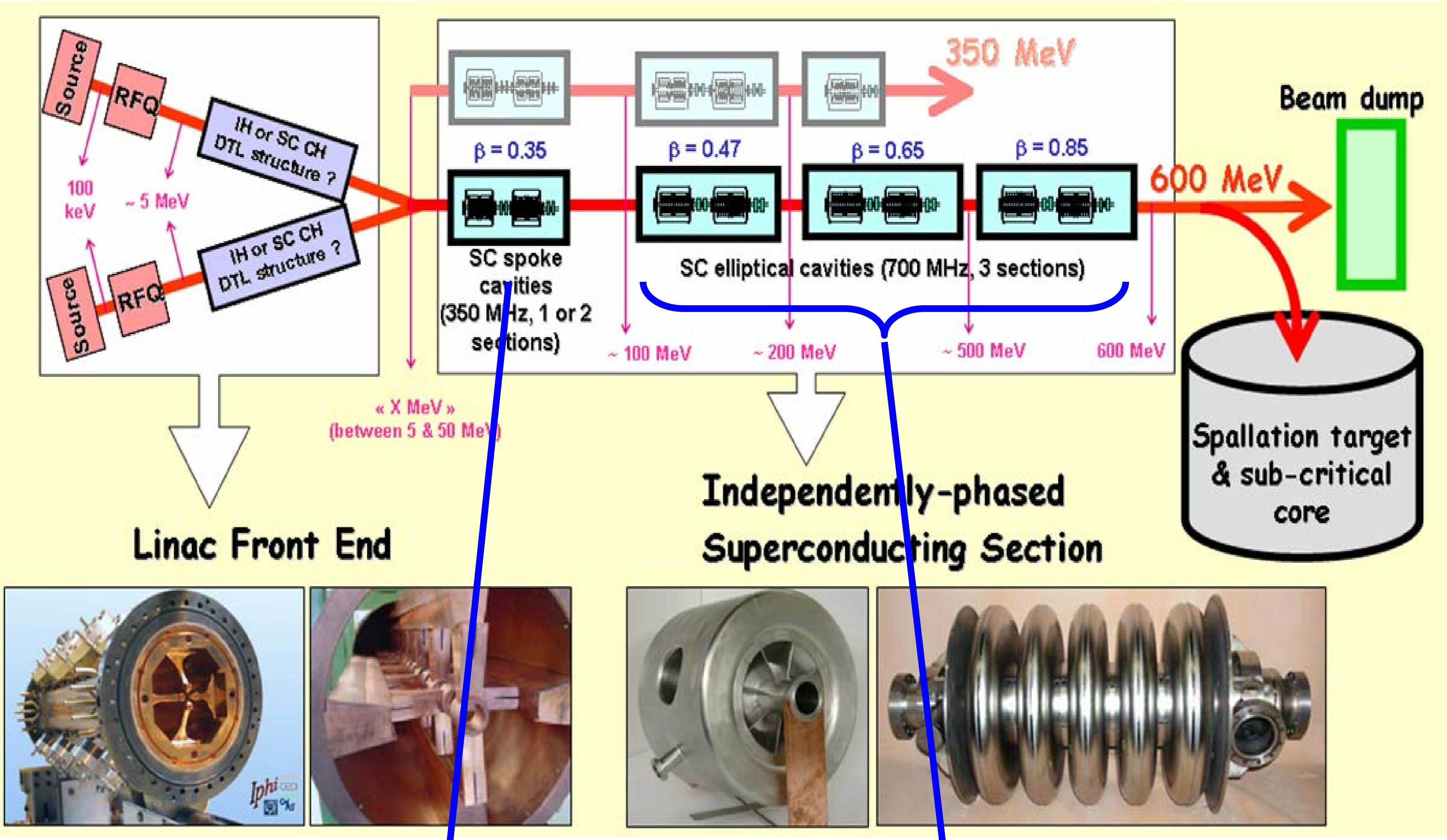
- We cannot rely on MTBF data sources for typical accelerator components (usually special components)

- The set of data is used to develop a system scheme that guarantees the proper reliability characteristics with the given components by using
  - fault tolerance capabilities
  - redundancy patterns

- Experimental activities foreseen within EUROTRANS will provide more knowledge on some of the reliability characteristics of the key components

- Also SNS operational experience is very relevant

EUROTRANS linac



96 RF units

92 RF units

Fifth International Workshop on the Utilisation and Reliability of High Power Proton Accelerators

Parts count

- With a “parts count” estimate we come to an obviously short MTBF ~ 30 h
- Split into:

Injector:	7.7%
Spoke linac:	45.4%
High energy linac:	43.5%
Beam line:	0.6%
Support systems:	2.7%

- Of course, the highest number of components is in the linac (nearly 100 RF units each, with each RF units having an MTBF of 5700 h...
- That already suggests where to implement strategies for redundancy and fault tolerance implementation

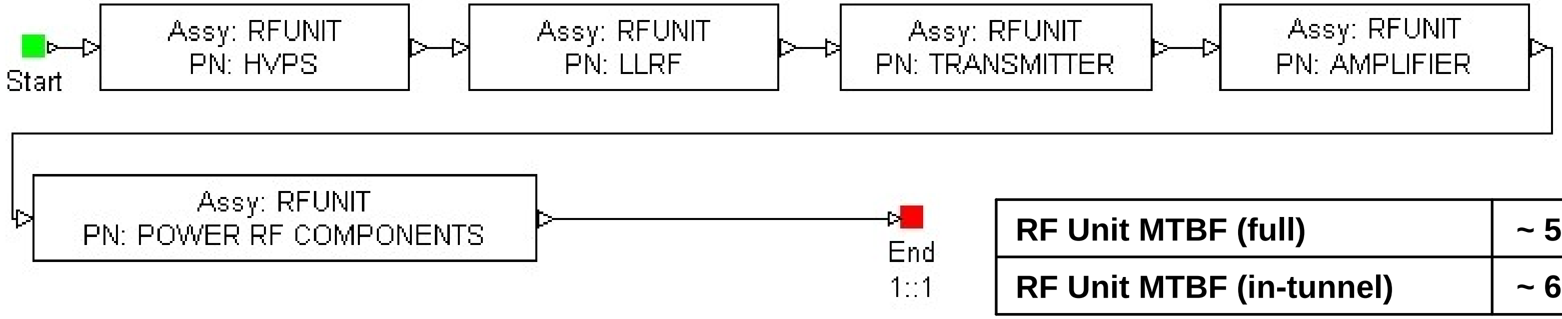
Subsystems

Injector

Support Systems

Standard support systems, with MTBFs only moderately tailored to mission time. Each system R(Mission time) = 0.48.

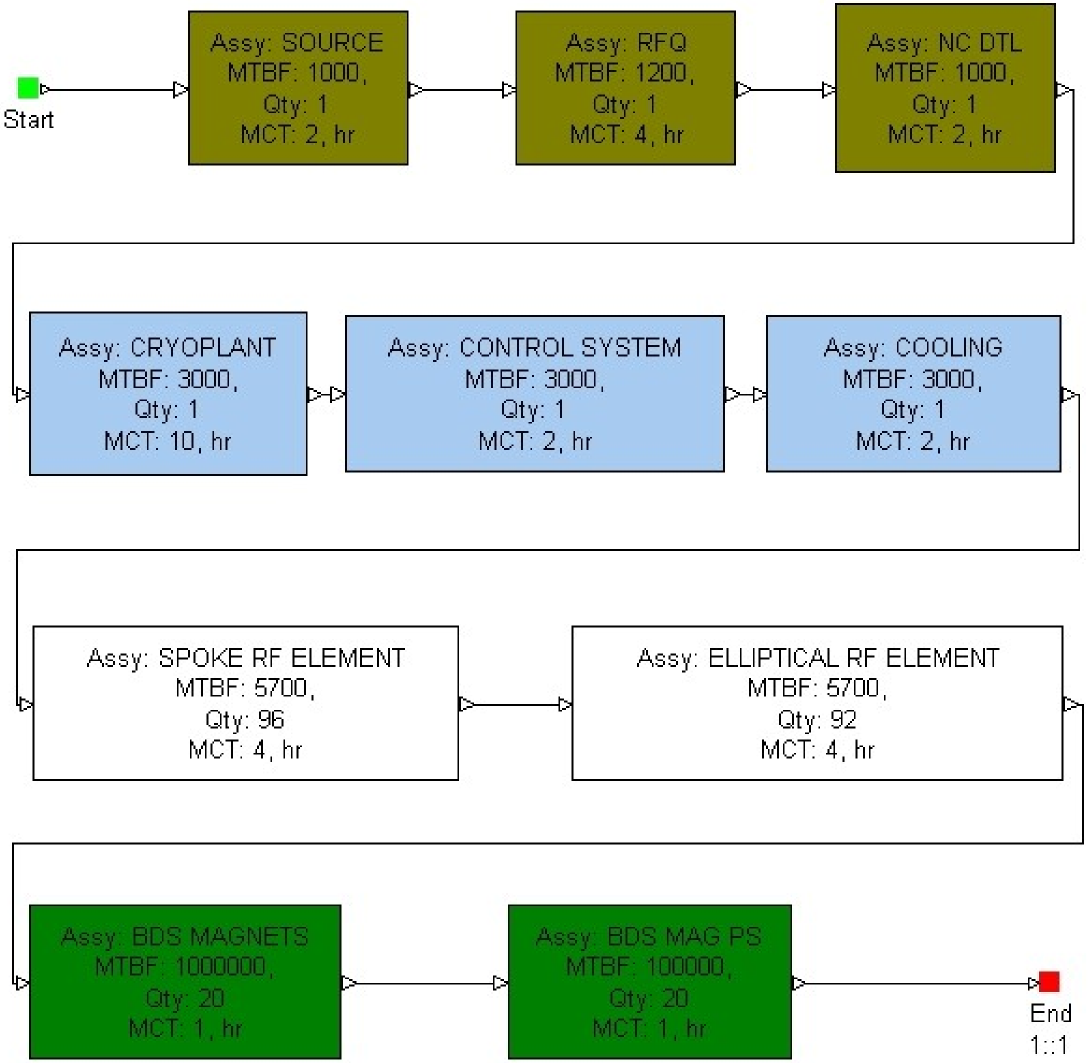
RF Units



RF Unit MTBF (full)	**~ 5700 hours**
RF Unit MTBF (in-tunnel)	**~ 6100 hours**

Initial Scenario – All Series, no redundancy

- Worst possible case
  - similar to parts count
- All component failures lead to a system failure
- Poor MTBF
- Too many failures per mission
- Mostly due to RF units
- 5700/188 = 30.32 h



Start

Assy: SOURCE
MTBF: 1000,
Qty: 1
MCT: 2, hr

Assy: RFQ
MTBF: 1200,
Qty: 1
MCT: 4, hr

Assy: NC DTL
MTBF: 1000,
Qty: 1
MCT: 2, hr

Assy: CRYOPLANT
MTBF: 3000,
Qty: 1
MCT: 10, hr

Assy: CONTROL SYSTEM
MTBF: 3000,
Qty: 1
MCT: 2, hr

Assy: COOLING
MTBF: 3000,
Qty: 1
MCT: 2, hr

Assy: SPOKE RF ELEMENT
MTBF: 5700,
Qty: 96
MCT: 4, hr

Assy: ELLIPTICAL RF ELEMENT
MTBF: 5700,
Qty: 92
MCT: 4, hr

Assy: BDS MAGNETS
MTBF: 1000000,
Qty: 20
MCT: 1, hr

Assy: BDS MAG PS
MTBF: 100000,
Qty: 20
MCT: 1, hr

End
1::1

System MTBF	**31.2 hours**
Number of failures	**70.23**
Steady State Availability	**87.2 %**

Mitigating occurrence of faults by system design

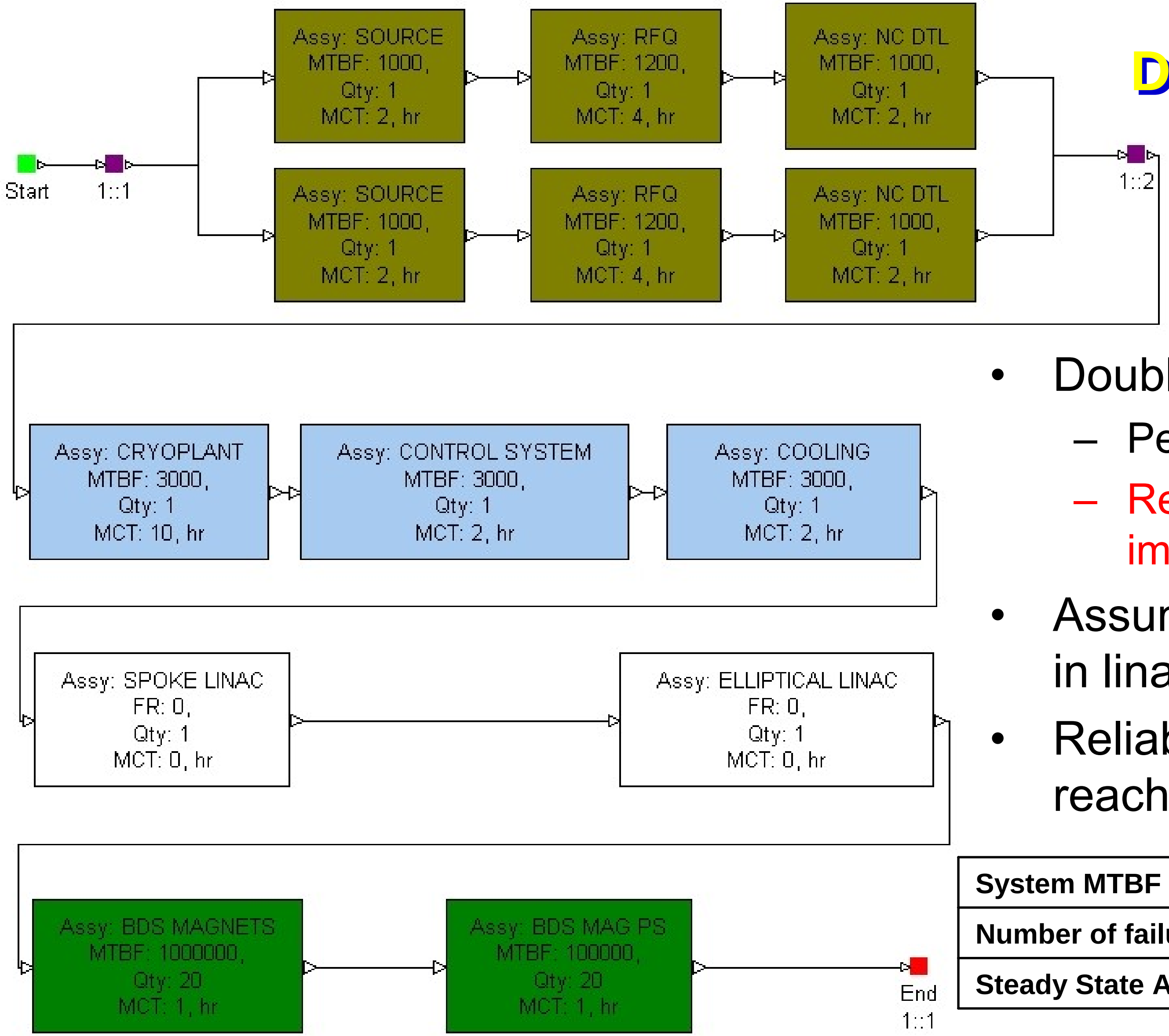
- Clearly, in the region where we are driven by *high number of moderately reliable components* we don't want a series connection (where each component fault means a system fault)
  - Need to provide **fault tolerance**

- Luckily, the SC linac has ideal perspectives for introducing tolerance to RF faults:
  - highly modular pattern of repeated components providing the same functions (beam acceleration and focussing)
  - individual cavity RF feed, digital LLRF regulation with setpoints and tabulated procedures

- In the injector low fault rates can be achieved by redundancy

2 Sources - ∞ Fault Tolerant SC section

Dream Linac



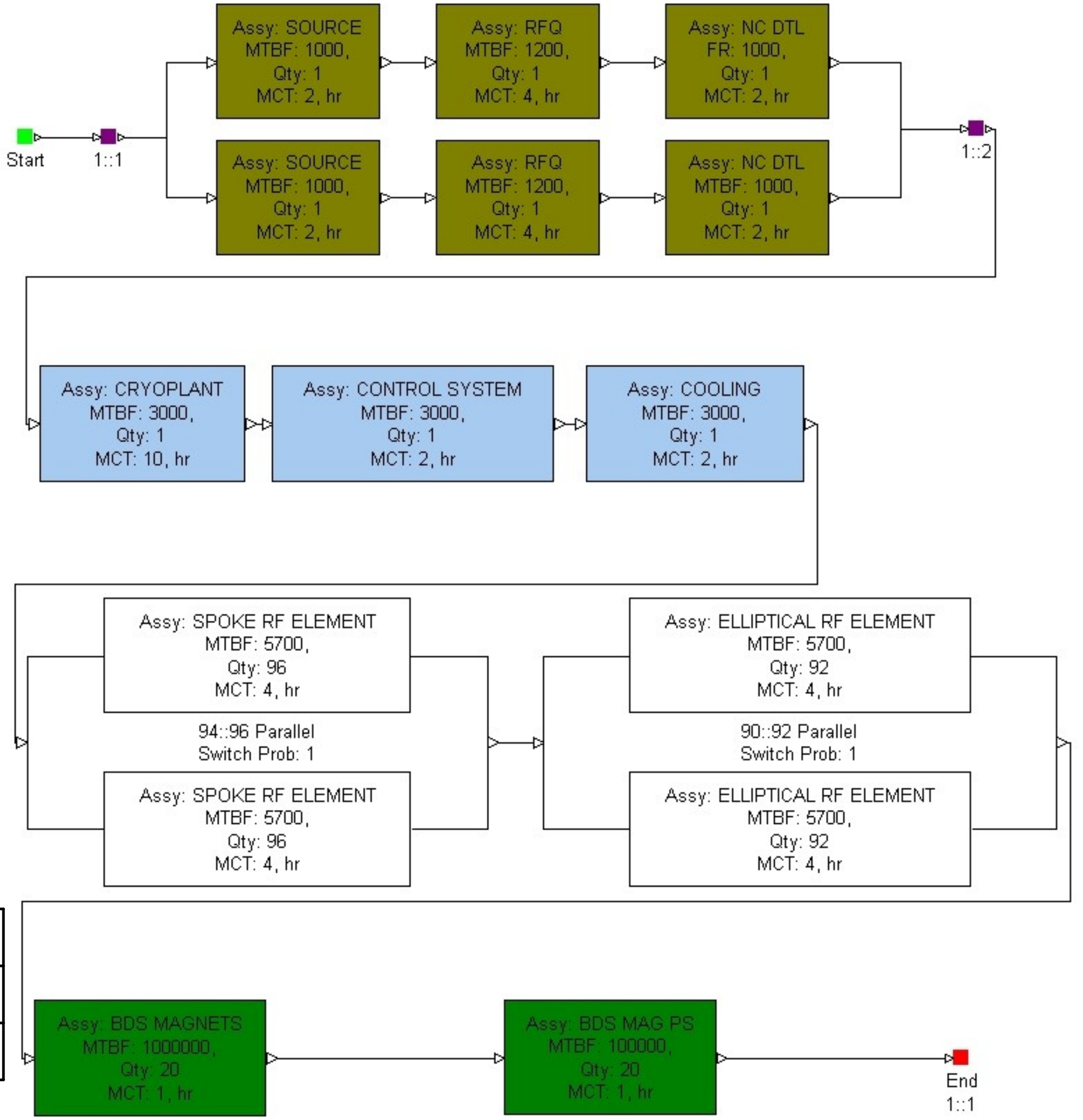
- Double the injector
  - Perfect switching
  - Repair can be immediate
- Assume infinite FT in linac section
- Reliability goal is reached!

System MTBF	796.91 hours
Number of failures	2.75
Steady State Availability	99.5 %

2 Sources – Redundant RF Systems

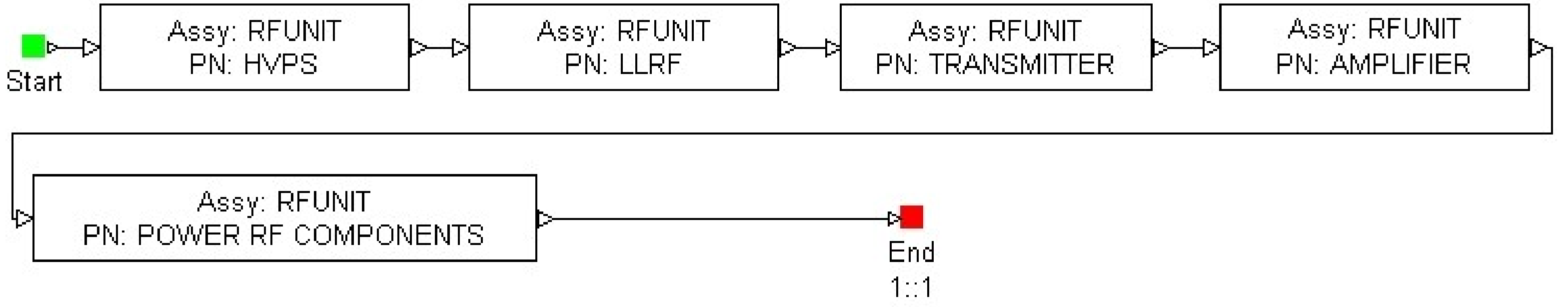
- Keep 2 sources
- Assume that we can deal at any moment with any 2 RF Units failing at any position in the SC sections
  - Maintenance can be performed on the failing units while system is in operation
  - ideal detection and switching
- Still within goals

System MTBF	**757.84 hours**
Number of failures	**2.89**
Steady State Availability	**99.5 %**



Realistic RF Unit correction provisions

- When assuming parallelism and lumped components we should be consistent in defining **repair provisions**
- For example, the components in the RF system that are out of the main accelerator tunnel **can be** immediately repairable, but certainly **not** all RF power components that are inside the protected-access tunnel
  - Even if the in-tunnel component can be considered in parallel (we may tolerate failures to some degree), all repairs are executed ONLY when the system is stopped
  - This greatly changes system MTBF



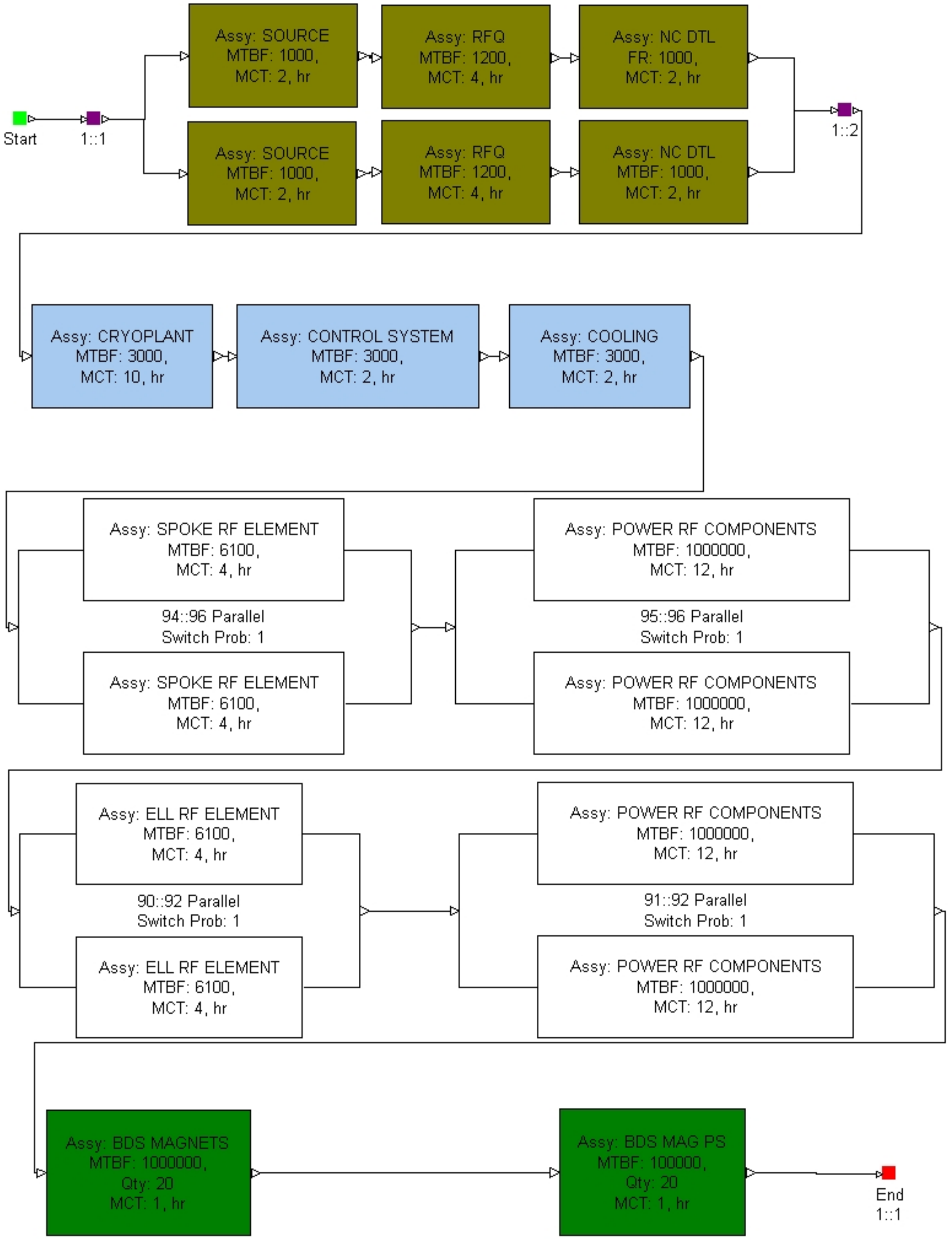
Final Scheme – Split RF Systems

- Keep 2 sources
- Split RF Units
  - Out of tunnel
    - Immediate repair
    - Any 2 can fail/section
  - In tunnel
    - 1 redundant/section
    - Repair @ system failure

System MTBF	**550 hours**
Number of failures	**3.8**
Steady State Availability	**97.9 %**

- Increasing only MTBFx2 of support systems

System MTBF	**720 hours**
Number of failures	**2.80**
Steady State Availability	**99.1 %**



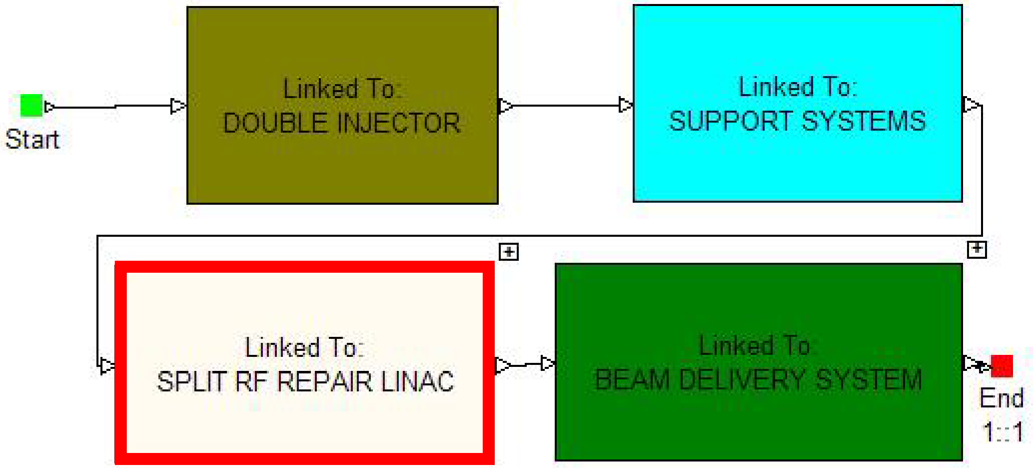
System MTBF “evolution”

# Inj.	Fault Tolerance degree	RF unit repair	System MTBF
1	None, all in series	At system stop	31
2	Infinite	Immediate	797
2	94/96 in spoke, 90/92 in ell are needed	Immediate	758
2	94/96 in spoke, 90/92 in ell are needed, more realistic correction provisions, by splitting the RF system	• Immediate for out of tunnel • at system stop for in tunnel	558
2	94/96 in spoke, 90/92 in ell are needed, split RF **SUPPORT SYSTEM MTBF * 2**	• Immediate for out of tunnel • at system stop for in tunnel	720
2	94/96 in spoke, 90/92 in ell are needed, split RF **IN-TUNNEL MTBF * 10**	• Immediate for out of tunnel • at system stop for in tunnel	760

Lesson learned

- Type of connection & corrective maintenance provisions change dramatically the resulting system reliability, independently of the component reliability characteristics
- This analysis allows to identify **choices of** components for which we need to guarantee high MTBF, due to their criticality or *impossibility of performing maintenance*
  - in-tunnel components/more robust support systems
- Analysis here is still crude, while similar MTBF values are reported in literature, the MTTR are inserted mainly for demonstration purposes
  - several issues ignored: decay times before repair, logistic issues, long times if cooldown/warmup is needed...

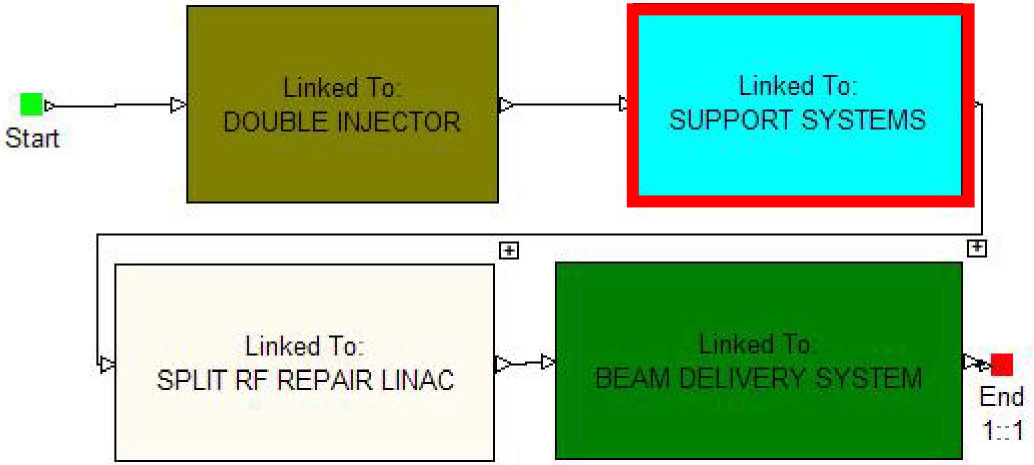
Example: acting on in-tunnel components



Here MTBF*10 in the in tunnel components

- In terms of fault rates in mission (2.9 total)
  - Injector contributes to 3%
  - Support systems amounts to 75%!
  - Linac is down to 5%
  - BDS is 17%
- Clearly longer MTBF in the conventional support systems is desirable...

Example: acting on support systems



Here MTBF*2 in the support systems

- In terms of fault rates in mission (2.8 total)
  - Injector contributes to 3%
  - Support systems amounts to 35%
  - Linac is 45%
  - BDS is 16%
- More balanced share of fault areas
- MTBF increase only in conventional support facilities

Fault tolerance

- Still, analysis assumes a high degree of fault tolerance, where the failure of an RF unit is automatically recovered without inducing beam trips on target in timescales ~ 1 s
  - challenging technical issue in LLRF and beam control systems

- Two tasks of the EUROTRANS accelerator program (Tasks 1.3.4 and 1.3.5) are dedicated to reliability analysis and LLRF issues for providing fault tolerance in the high power linac

Conclusions

- Even in the absence of a validated reliability database for accelerator components the standard reliability analysis procedures indicate where design effort should be concentrated:
  - providing large degree of fault tolerance whenever possible
    - Meaning: fault detection, isolation and correction procedures
  - providing additional design effort aimed at longer MTBF only in critical components

- Study here is an illustration of how, with minimal “tweaking” of the component MTBF, a simple model for an accelerator system can be altered (adding redundancy and fault tolerance capabilities) in order to meet the ADS goals