SDP Memo 43: Pulsar Timing Failure Analysis

Document Number ..... SDP Memo 43
Document Type ..... MEMO
Revision C1
Author ..... R. J. Lyon, L. Levin, B. W. Stappers
Release Date 2018-04-17
Document Classification ..... Unrestricted
Status ..... Draft

Lead Author	Designation	Affiliation
R. J. Lyon	SDP.PIP.NIP Member	University of Manchester
Signature & Date:	(17/04/2018)	

SDP Memo Disclaimer

The SDP memos are designed to allow the quick recording of investigations and research done by members of the SDP. They are also designed to raise questions about parts of the SDP design or SDP process. The contents of a memo may be the opinion of the author, not the whole of the SDP.

Revisions

Revision	Date of issue	Prepared by	Comments
C	February 26th 2018	Robert Lyon	Initial version of the document.
C1	April 17th 2018	Robert Lyon	Updates made given feedback from Lorita Christelis. Updated Tables 5 and 6, replaced some text that was incorrectly repeated. Altered Table 4. making it clear that FM.SDP.PST.103 can also be mitigated via rerouteing data to functioning hardware. Added a new mode, FM.SDP.PST.117, to account for a hardware failure in the archive system. Altered Table 5., making a grammatical change to FM.SDP.PST.108 in the mitigation column (no change to meaning). Section 5.2, indicated that a rack control failure can occur due to the failure of a top of rack switch. Section 5.2, indicated that a loss of control due to failure of the SDP management system, unlikely to be cause by a loss of connectivity. There will likely be a network topology that ensure a connection is always available, though perhaps with reduced bandwidth.

			Continued... Section 5.2, now point to the SDP execution control component [RD9] (see section 2.1.1 in that external document) as a possible source of failure. Modified FM.SDP.PST.205 and FM.SDP.PST.206 in Table 7. Added an additional mitigation strategy, which involves decoupling control and monitoring in the SDP Execution Control Component. Altered Table 11., making it clear that FM.SDP.PST.224 has the potential to critically impact science outputs, rather than catastrophically degrade output. Also updated the severity range and the criticality score. This is because the failure mode can be mitigated so long as science data is retained in a buffer and not discarded until successfully persisted in the archive. Added new tables to the Appendix that describe FMECA Detection methods. The following changes have been made to the requirements in Table 25: SDP_REQ-33 has a new description. SDP_REQ-50 has since been deleted. SDP_REQ-147 and SDP_REQ-148 have since been deleted. SDP_REQ-281 has a new description. SDP_REQ-546 has a typo correction. SDP_REQ-552 has since been deleted. SDP_REQ-763 has a new description. SDP_REQ-764 has a new description.

Table of Contents

List of Figures

List of Tables

List of abbreviations

CSP	Central Signal Processor
COTS	Commercial-of-the-Shelf
DSD	Dynamic Spectra Data
EMI	Electromagnetic Interference
FTP	File Transfer Protocol
HPC	High Performance Computing
ICD	Interface Control Document
IM	Interstellar Medium
LMC	Local Monitor and Control
NIC	Network Interface Card
NIP	Non-imaging Processing
PSRFITS	Pulsar Flexible Image Transport System
PST	Pulsar Timing Sub-element
PTD	Pulsar Timing Data
QA	Quality Assurance
SDP	Science Data Processor
SFMECA	Software Failure Mode, Effects and Criticality Analysis
TM	Telescope Manager
TOA	Time-of-Arrivals
TOR	Top of Rack

Summary

This document describes a Software Failure Mode, Effects and Criticality Analysis (SFMECA) for the pulsar timing pipeline sub-element (PST) of the Science Data Processor (SDP). The analysis has been done at the architectural level, and represents an initial attempt to study the failure modes of the timing pipeline. This work forms the output of sprint task: TSK-2140.

Applicable Documents

The following documents are applicable to the extent stated herein. In the event of conflict between the contents of the applicable documents and this document, *the applicable documents* shall take precedence.

Reference Number	Document Number	Reference
AD1	100-000000-002	SKA1 LOW SDP - CSP INTERFACE CONTROL DOCUMENT
AD2	300-000000-002	SKA1 MID SDP - CSP INTERFACE CONTROL DOCUMENT
AD3	100-000000-029	SKA1 INTERFACE CONTROL DOCUMENT SDP TO TM LOW
AD4	300-000000-029	SKA1 INTERFACE CONTROL DOCUMENT SDP TO TM MID

Reference Documents

The following documents are referenced in this document. In the event of conflict between the contents of the referenced documents and this document, *this document* take precedence.

Reference Number	Document Number	Reference
RD1	SKA-TEL-SDP-0000018	PDR.02.01 Compute Platform Element Subsystem Design
RD2	SKA-TEL-SDP-0000027	SDP Pipelines Design
RD3	SKA-TEL-SDP-0000033	SDP L2 requirements specification (L1 Rev 11).
RD4		Zhu, Y. M., "Software Failure Mode and Effects Analysis", Springer, 2017, doi:10.1007/978-3-319-65103-3_2.
RD5		Stadler, J. J. and Seidl, N. J.,"Software failure modes and effects analysis", Reliability and Maintainability Symposium (RAMS), 2013, doi:10.1109/RAMS.2013.6517710.
RD6		Stamatis, D. H., "Failure mode and effect analysis : FMEA from theory to execution", Milwaukee, Wisc. : ASQ Quality Press, 2003.
RD7	SDP Memo 40	Lyon, R. J., Levin, L. and Stappers, B. W., "PSRFITS Overview for NIP".
RD8		Lyon, R. J., "CSP to SDP NIP Data Rates & Data Models (version 1.1)", doi:10.5281/zenodo.836715.
RD9	SKA-TEL-SDP-0000013	Wortmann, P. et. al., "SDP Operational System Component and Connector View ".

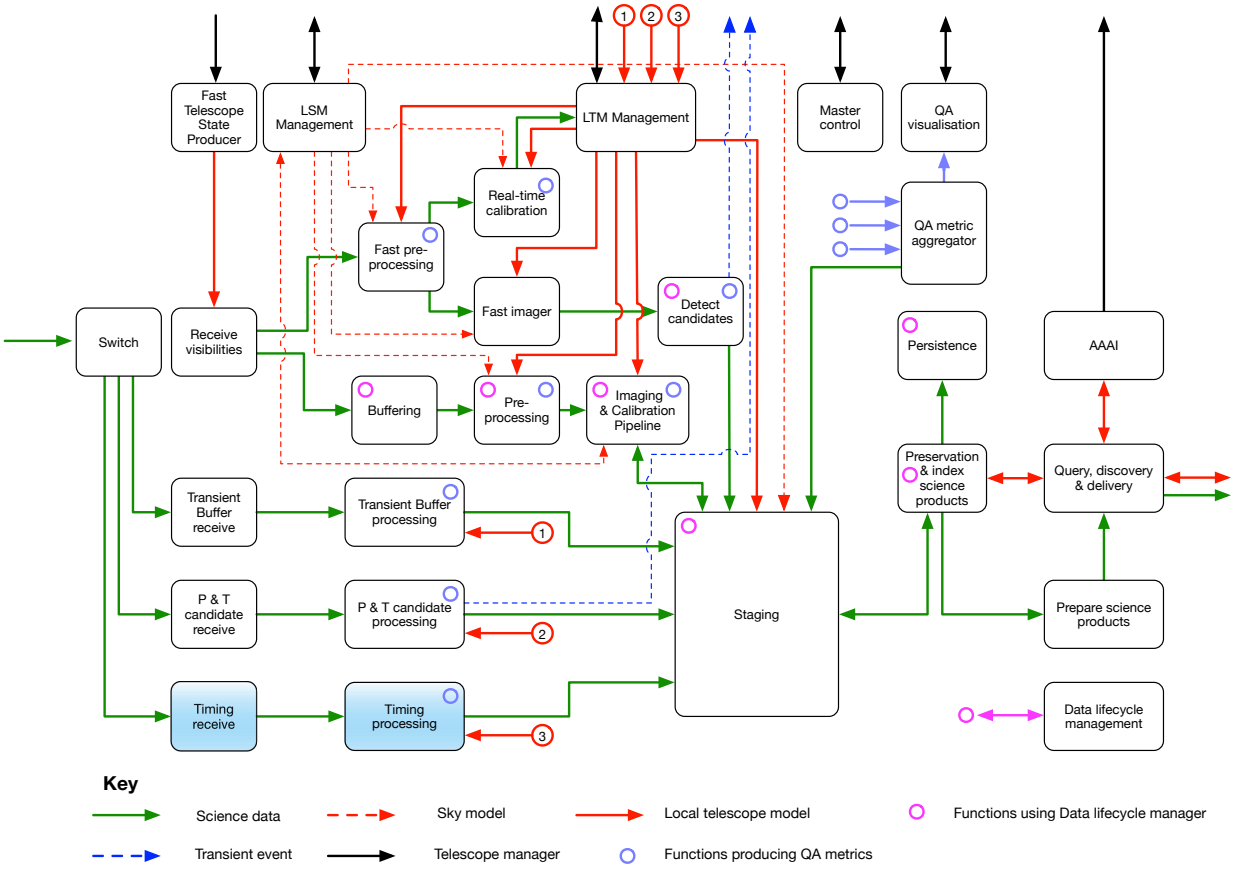

Figure 1: Level 2 functional flow diagram for the SDP. The blue shaded components are those studied as part of the failure analysis. The flow diagram is based upon a figure produced by the SDP consortium (author unknown).

1 Scope

The scope of this work is confined to the blue shaded components of the SDP level 2 functional flow diagram in Figure 1. This includes the pulsar timing receive and pulsar timing functions, from herein collectively referred to as the SDP.PST. The analysis presented here is only concerned with the identification and analysis of SDP.PST software failure modes at an architectural level. The analysis is applicable to both SKA Low and Mid. It includes failure modes arising from internal and external software (and their interfaces), firmware, interfaces to Commercial-of-the-Shelf (COTS) equipment, and interfaces to free/open source software. Whilst hardware failure modes are not in scope, in some cases hardware will be discussed when equipment failures, faults, or defects precipitate software failures/errors. As the SDP design is not complete, hardware, software and architectural assumptions are made to both enable and constrain the analysis. These assumptions are summarised in Section 4, whilst the methodology employed is summarised and justified in Section 2. Finally, note that the pulsar and transient search Non-Imaging Processing (NIP) pipeline failure modes will be considered elsewhere.

2 Process

Whilst software failure mode analyses have been undertaken for some time, there is currently no universal SFMECA standard. To proceed it is necessary to tailor approaches borrowed from the software engineering literature. Thus we reviewed the literature [RD4,RD5,RD6] for relevant work. Following this review we designed a process we believe to be conducive to producing a reproducible, principled, detailed analysis. This is an initial attempt to systematise the SFMECA so that it can be reviewed and critiqued, and we hope that our process can be improved upon via appropriate feedback. Any such feedback will be incorporated into future SFMECA analyses, e.g. those yet to be done for the pulsar and transient search pipelines.

The following steps form the analysis process employed in this work:

1. **Define the scope** - This involves determining i) which part of the system is being investigated, ii) which views apply (e.g. functional, interface, algorithmic, maintenance, usability, security), iii) which elements to study (e.g. hardware, software).

2. **Information gathering** - Gather documents relevant to the analysis, e.g. if taking a functional view then requirements documents are relevant. This is because failures lead to functional requirements not being met. Interfaces may need to be studied, along with the system functionality at a higher level. This also involves studying which types of analysis can be applied - an SFMECA process designed for medical software, will have different strengths and weaknesses compared to one written for military applications. Thus it's important to find the right approach.

3. **Tailor the analysis** - Based on the information gathered, tailor the analysis to the problem at hand. In this case, we need not consider hardware failure modes, thus we can omit these from the analysis.

4. **Research failure modes** - Enumerate all the possible failure modes and sources of error. Then begin categorising these according to the chosen view.

5. **Analyse** - For each mode found determine,

    - the root cause of the failure mode.
    - the local effect at the software component level (e.g. FFT doesn't work correctly).
    - the sub-system effect. For example the effect on the pulsar timing pipeline subsystem.
    - the system effect and how this relates to system requirements (e.g. if pulsar timing fails, what does this mean for SDP, and the wider SKA?).

6. **Mitigate** - For each failure mode identified, attempt to devise a mitigation strategy which prevents the failure or mitigates its effects. If no mitigation is possible, then preventative measures should be described.

7. **Severity & Likelihood** - Determine how severe each failure mode is with respect to the system requirements, and how likely it is for such a failure mode to occur.

8. **Summarise** - Produce a critical item list describing all the possible failure modes.

These steps need not be rigidly undertaken. However they are useful for guiding the analysis process. Note these steps are described in more detail elsewhere [RD4,RD5,RD6].

Table 1: Severity codes applying to failure modes.

Level	Code	Description
1	Minor	Normal availability retained by preventative / mitigation action.
2	Marginal	Near normal availability retained via preventative / mitigation action.
3	Significant	Operating between degraded and normal.
4	Critical	Operating in degraded mode.
5	Catastrophic	Functionality unavailable.

Table 2: Likelihood codes applying to failure modes.

Level	Code	Description
1	Extremely unlikely	$< 0.1\%$
2	Remote	0.1 to 1%
3	Occasional	1 to 10%
4	Reasonably probable	10 to 20%
5	Frequent	$>$20%

3 Terms & Definitions

Before proceeding we define some terms which should make our analysis easier to interpret. Firstly we define the severity codes (Table 1) and probability codes (Table 2) that will be used. These are used to determine a criticality level for each failure mode. The criticality score can be determined via a simple calculation where the *Criticality Score* $=$ *Severity* $\times$ *Likelihood*.

Next we define the key terms as we understand them.

- **Failure Mode** - Means/process via which software can contribute to a system failure.
- **Effect** - Behaviour resulting from the failure mode.
- **Error** - Discrepancy between a computed, observed, or measured value and the *true*, specified or theoretically correct value or condition.
- **Defect** - Manifestation of an error arising from the software requirements, design or code.
- **Fault** - Defect that has resulted in one or more failures.
- **Scan** - Basic observational unit.

4 Assumptions

4.1 Hardware

The SDP.PST pipeline is assumed execute upon standard COTS equipment that complies with the SKA's EMI, power, maintenance and cooling standards. This applies to racks, routers & switches, compute nodes and individual (internal) compute node components (processors, memory, accelerator cards, storage disks, NICs, power supplies, cooling components etc). The hardware is assumed to be housed in a suitable location providing appropriate power, cooling and climate control facilities. Figure 2 depicts our hardware assumptions. An abstracted rack configuration presented in a), and an abstracted SDP compute node in b).

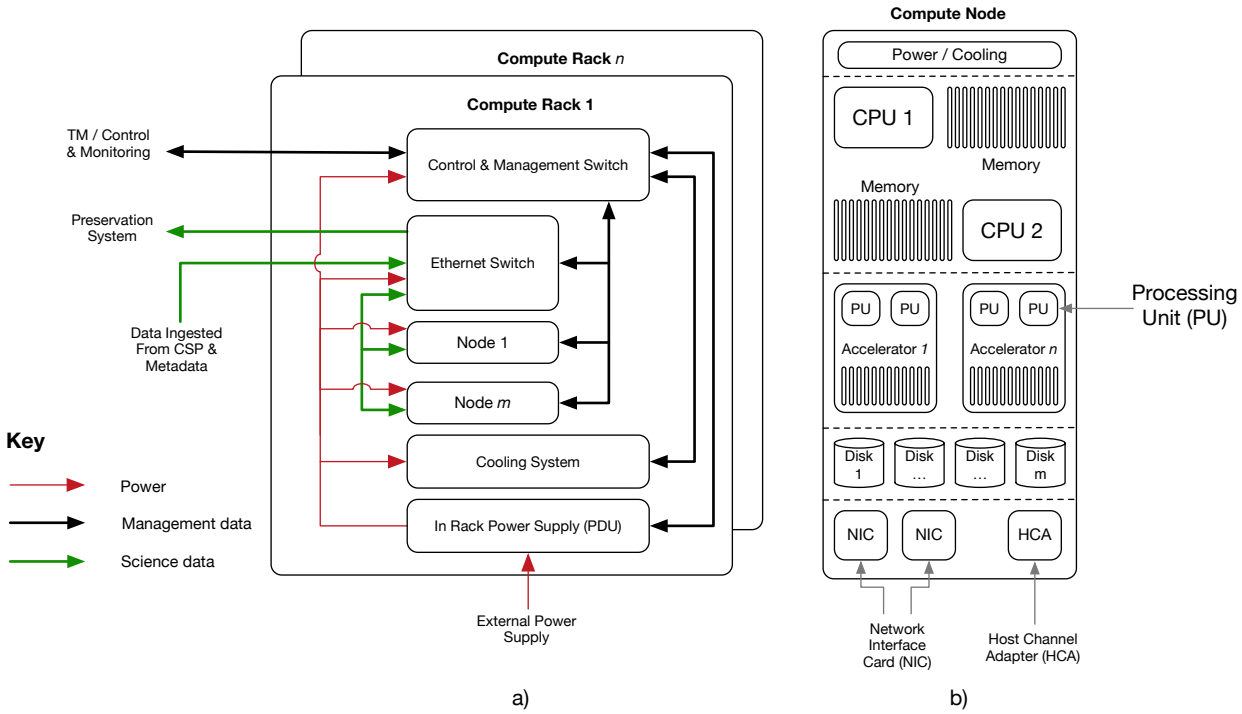

Figure 2: Simplified hardware block diagram describing SDP racks (a) and a diagram depicting an abstracted SDP compute node (b). Figure based upon diagrams originally produced by L. Christelis and P. C. Broekema, as part of their SDP work.

4.2 Architecture

The SDP will be an energy efficient yet extremely powerful High Performance Computing (HPC) system. We assume it consists of one or more 'compute islands'. Each compute island is an independent scalable compute unit[1] [RD1] containing one or more racks as shown in Figure 2 a). Each rack can in turn contain one or more compute/data storage nodes. Where a compute/data storage node is a typical COTS server as shown in Figure 2 b). In addition to COTS servers, each rack is presumed to contain industry standard networking and storage hardware.

[1]Compute islands defined in JIRA, see Archive 390: `https://jira.ska-sdp.org/browse/ARCHIVE-390`.

Based on these assumptions we describe an abstracted architecture used to guide our analysis. It is summarised in the architectural data flow diagram shown in Figure 3. We assume that,

- each rack, and each compute node within it, is connected to a control system via a 'management' Ethernet switch. The control system is responsible for provisioning resources within the rack, monitoring their use, troubleshooting etc.
- each rack has a separate Ethernet switch dedicated to handling the ingest/transmission of all other data (e.g. science data, sky models, and metadata). Each compute node is connected to this switch, allowing data to be received from the CSP, and sent to the preservation system as appropriate.
- rack power and cooling is monitored via the management system.
- compute islands, the Telescope Manager (TM), the Central Signal Processor (CSP) and the preservation system; are connected via suitable network interfaces and equipment.
- there will be redundant compute nodes, data storage nodes, and communication links which will help mitigate the impact of hardware failures.
- for our analysis we can treat the TM, CSP and preservation systems as black boxes interacting with our pipeline components. Thus any failure modes related to their use can only occur at any applicable common interfaces.

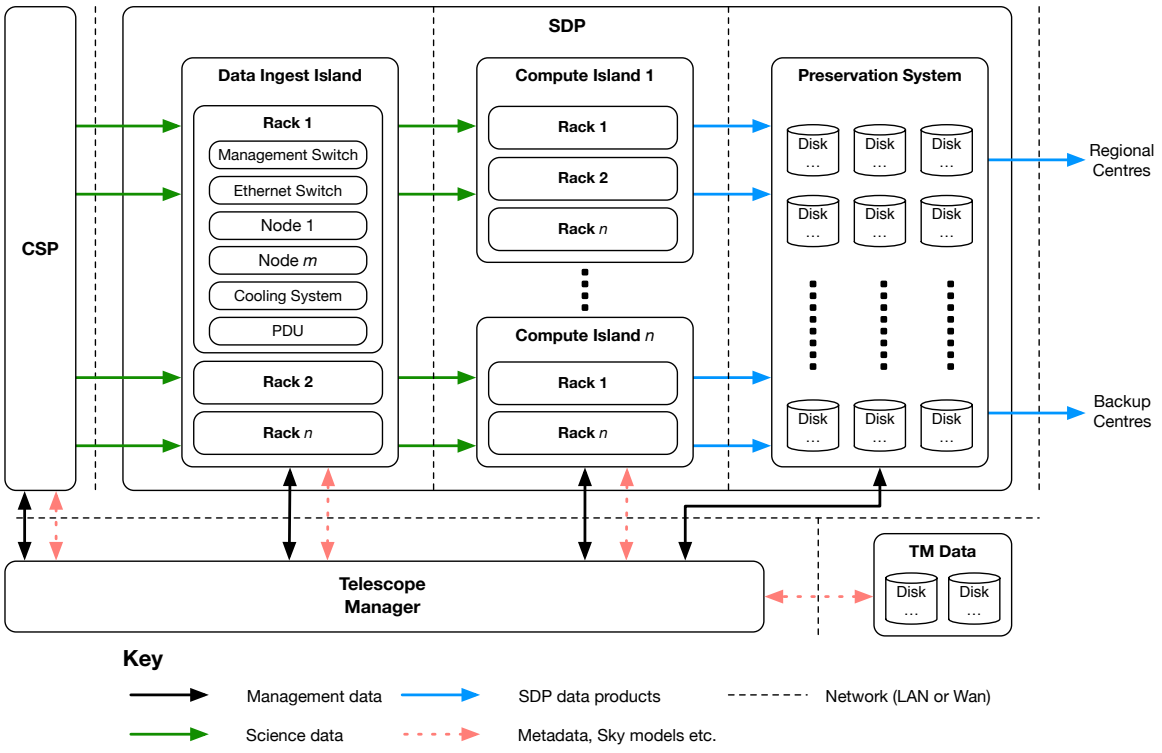

Figure 3: High level diagram showing the assumed architectural data flow. Figure based upon diagram first presented in [RD1].

4.3 Control

We treat the control system as a single abstracted entity interacting with the SDP.PST, and SDP hardware. For this analysis it is irrelevant if control is provided by the TM (e.g. [AD3,AD4]), LMC (Execution Control) or direct human interaction so long as,

- the control system initiates, pauses, and restarts scan processing as appropriate.
- the control system monitors both hardware and software states allowing the efficient management of resources.
- the control system can receive and correctly process information requests from the SDP.PST or the SDP.
- the control system can deliver information to the SDP.PST or the SDP. This includes details of the processing to be performed, associated metadata, sky models, pulsar ephemerides, standard pulsar profiles, RFI masks, calibration strategies and other relevant information.
- the control system can process and correctly act upon error messages/warnings sent by the SDP.PST or the SDP.
- the control system has some inherent redundancy making failures of the control system extremely unlikely.
- the control system can operate autonomously during scan processing, and take remedial action where/when appropriate according to any error messages received. This includes, for example, automatically compensating for hardware failures at the node level.

4.4 Communications

As per the CSP to SDP Interface Control Documents [AD1,AD2], we assume data is transmitted to the SDP via FTP (RFC 959). The communication interface is assumed to be bi-directional, although the data flow is uni-directional in practice (from CSP to SDP). Pulsar timing data transmitted via this protocol is sent one temporal sub-integration at a time[2] typically every 10 seconds. Though sub-integration data could be sent by CSP at any interval between 1 to 60 seconds. Finally the sub-integration data is sent in the PSRFITS format [RD7].

4.5 Execution Framework

The execution framework is responsible for executing software components, providing them with hardware resources (memory, CPU time etc), monitoring their status/resource use, and restarting them upon failure. The framework treats available hardware resources as a pool, thus processing steps executed one after another need not be situated on the same physical hardware. It is the responsibility of the execution framework to correctly route data from one software component to another, if executed on different hardware. Finally the execution framework interacts with the control system and is situated on each and every SDP node.

[2] Defined more clearly in Section 4.7.

4.6 Science Software & Processing

Science software is expected to comprise both custom tools developed by the SDP consortia, and open source community algorithms. In either case, these will operate within the constraints of the execution framework, and interface with its error reporting system, so that errors can propagate from all software components to the TM.

Pulsar timing processing proceeds in a mostly linear fashion, with some data aggregation/buffering required in places. It is entirely possible for the processing to be done across multiple racks and/or compute islands. However it is better for data from the same beam to be processed on the same physical compute node.

4.7 Data

The CSP produces 'detected' data. This is data that has been i) channelised, ii) fully corrected for dispersion in the Interstellar Medium (IM), iii) folded at the known pulsar period, and iv) partially calibrated. The resulting time, phase, frequency and polarisation data is sent to the SDP.PST as a matrix (also called a data cube). The matrix dimensions are determined by parameters chosen within CSP. These include the number of frequency channels N_{chan}, the number of phase bins N_{bin}, the number temporal sub-integrations N_{sub}, and the number of polarisations N_{pol}. The size of the matrix in bits is given by,

$$N_{chan} \times N_{bin} \times N_{sub} \times N_{pol} \times N_{bit}, \tag{1}$$

where N_{bit} is the number of bits per sample in the matrix. The possible values for these parameters are constrained elsewhere [AD1,AD2]. The data cube is not sent alone. It is accompanied by attributes and metadata. We describe the complete data product that contains all this information as Pulsar Timing Data (PTD). This is described at the conceptual level in Figure 4 and summarised elsewhere [RD8].

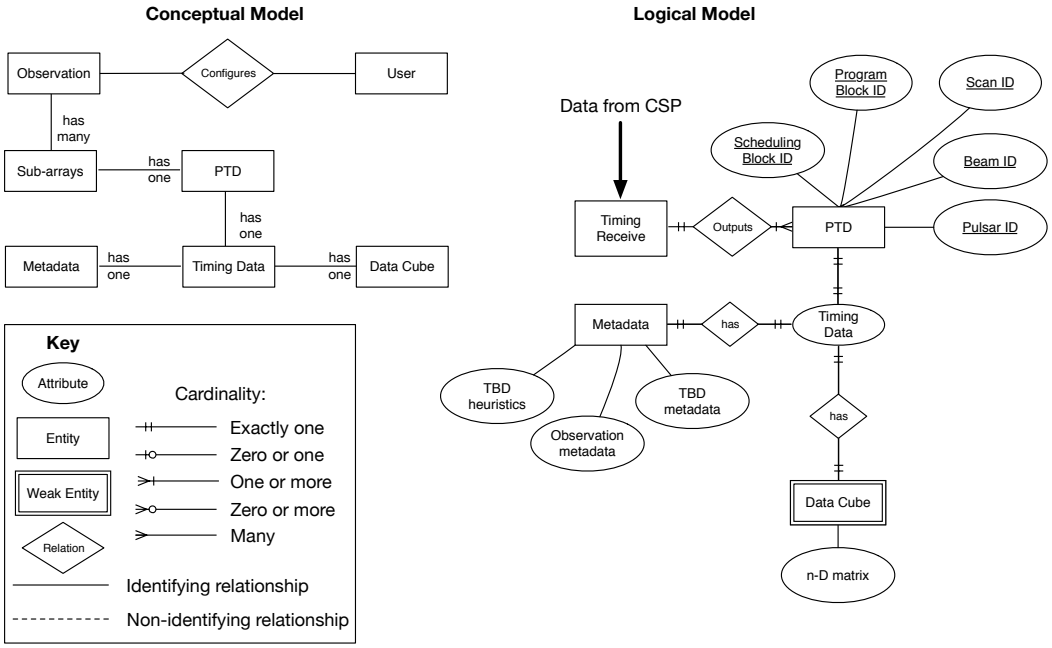

Figure 4: Conceptual data model for timing data.

Table 3: Summary of the main SDP.PST software components.

Identifier	Name	Description
SDP.PST.SC001	Command QA	Evaluates the quality and correctness of received commands.
SDP.PST.SC002	Parameter QA	Evaluates the quality and correctness of received parameters.
SDP.PST.SC003	Data QA	Evaluates the quality and correctness of received data, and data produced within the pipeline.
SDP.PST.SC004	Alert	Generates, formats and transmits alert messages. This includes scientific and hardware/software related alerts/warnings.
SDP.PST.SC005	Timing Receive	Monitors and controls the ingest of data from the CSP.
SDP.PST.SC006	Remove RFI	Removes parts of the received data affected by RFI.
SDP.PST.SC007	Calibrate	Calibrates for flux and polarisation.
SDP.PST.SC008	Average	Produces partly averaged data cubes for data processing steps that require higher S/N values rather than high resolution. Sends averaged products to the preservation system.
SDP.PST.SC009	TOA Determination	Determine pulse TOAs by cross correlating the current observation, with a pulsar-specific standard profile supplied externally. Generates 1 TOA per sub-integration and frequency channel.
SDP.PST.SC010	Compute Residuals	Uses a timing model to compute expected pulse TOA. Compares the expected & observed TOA, and generates timing residuals as the difference between them.
SDP.PST.SC011	Update Timing Model	Update the timing model for the observed pulsar.

4.8 Pulsar Timing Modes

A maximum of 16 tied-array beams are available for use when in pulsar timing mode. Each beam can independently observe a different pulsar, thus 16 pulsars can be studied per scan. It is the responsibility of the CSP to produce data products that can be used by the SDP to perform high precision timing.

The SDP.PST executes multiple processing steps. The first involves RFI mitigation followed by a detailed flux and polarisation calibration. A number of intermediate 'averaged' data products are then generated, that provide different representations of the data. These are sent to the preservation archive. The pulse Time-of-Arrivals (TOAs) are then determined, and the timing residuals computed. These are used to update the timing model for the observed pulsar following appropriate Quality Assurance (QA) checks. Any significant changes in pulse arrival times should raise an alert, as such a change is of scientific interest. The generalised pipeline steps are summarised in Figure 5, whilst Table 3 summarises the main SDP.PST components.

Note that all software components must be fault tolerant. To achieve this the timing pipeline must be capable of operating in two distinct modes:

- **Standard mode** - here communications are consistent, all data sources are accessible, all data sent and received is correctly formatted and valid, and data is successfully passed between SDP.PST software components without impediment (e.g. delays).
- **Default mode** - in the event of any error causing i) a disturbance in communications, ii) command parameters or metadata to become corrupted/invalid, iii) data formatting errors/corruption, iv) algorithmic/hardware malfunctions, v) a failure in control, or vi) any other unforeseeable error; the timing pipeline should enter a default mode. This mode prioritises the preservation of valuable science data, and may skip some/all processing steps as required.

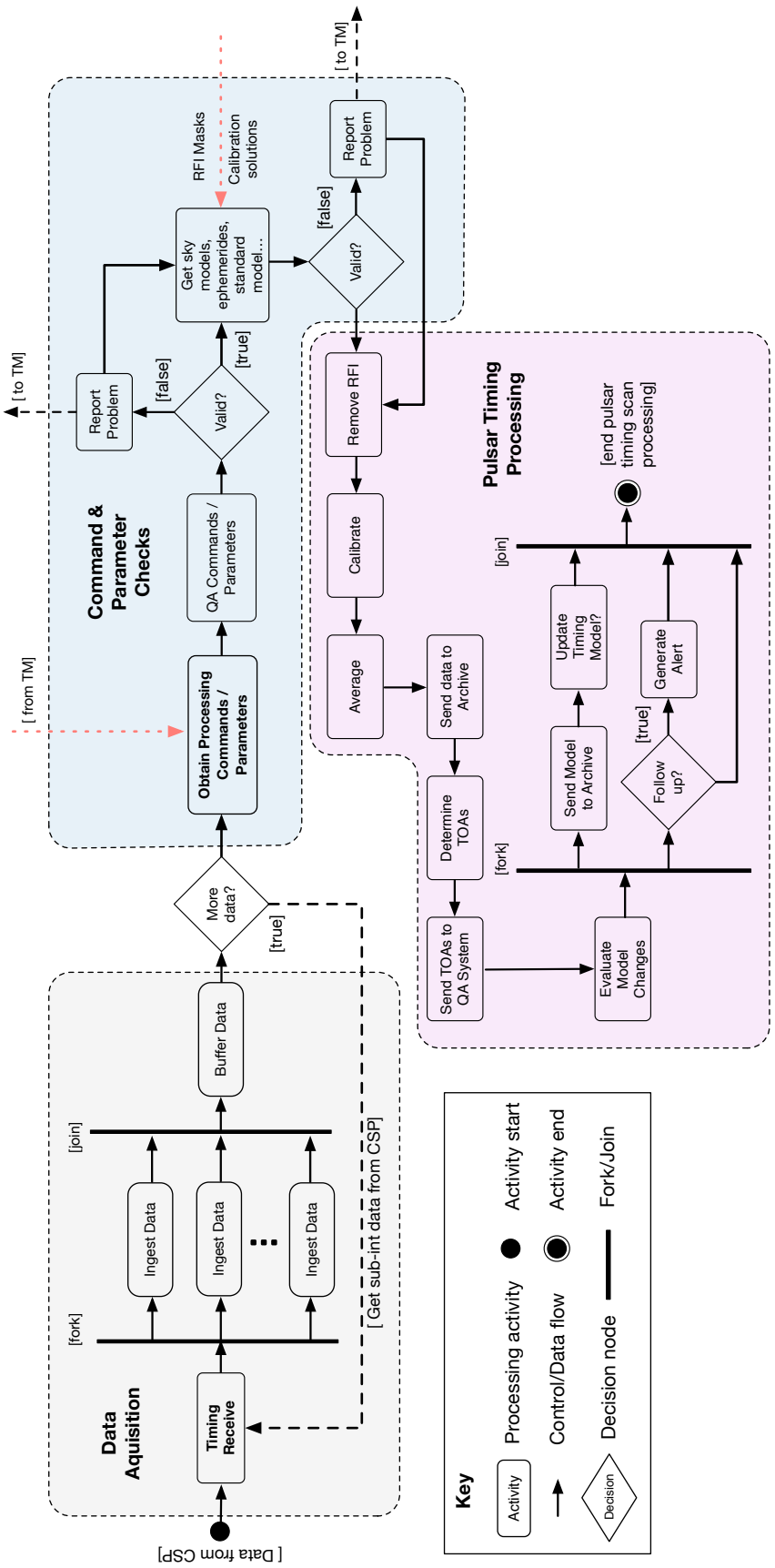

Figure 5: Activity diagram showing the processing steps in the pulsar timing pipeline.

4.9 Likelihood & Probability

The likelihood and probability estimates provided by this analysis represent best guesses based on empirical experience. Whilst this is not ideal, there is no data available that can be used to facilitate a more rigorous analysis of failure rates and consequences.

5 Failure Modes

We consider three main sources of failure. These are addressed in separate sections for clarity. In each case the priority is to preserve science data whenever possible, even when extreme errors are encountered. This is because science data, even when damaged or corrupted, has utility.

5.1 Hardware Induced Failures

There are many possible causes for a hardware induced failure. These can occur before and during timing processing. To keep the analysis at a high-level, we consider the following hardware failures and treat them as equivalent:

- failures resulting from a mechanical defect (e.g. system fan or hard drive mechanical failure).
- power or cooling failures necessitating system shut-down.
- failures caused by incorrect system configuration (e.g. Bios errors).
- failures caused by firmware or operating system errors.
- electronics failures in hardware components (memory, CPU, motherboard etc.).

A number of failure modes related to hardware errors are listed in Tables 4, 5 and 6 below. For simplicity only scenarios where inherent redundancy fails are presented (i.e. a worst case scenario). This is because enumerating all possible failure scenarios and their combinations is out of scope for our high level analysis.

Table 4: Hardware induced failure modes 1-6.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Timing Receive (FM.SDP.PST.101)	The SDP hardware responsible for ingesting data from the CSP encounters a hardware failure at the node level.	An ingest failure results in data loss at the sub-integration data level or for an individual beam, and delays the processing.	Pulsar timing analysis less effective, some science data lost.	Operational reliability and efficiency are degraded. Integrity of Science Data is compromised due to data loss.	Ensure the regular maintenance of ingest nodes, and prevent their use when exhibiting behaviours symptomatic of an impending hardware failure. Where possible immediately compensate for the error by repeating the ingest with operational hardware.	Minor	Occasional
Timing Receive (FM.SDP.PST.102)	The SDP hardware responsible for ingesting data from the CSP encounters a hardware failure at the rack level.	An ingest failure results in significant data loss for one or more beams, and significantly delays the processing.	Pulsar timing analysis significantly compromised, moderate science data lost.	Operational reliability and efficiency are degraded. Integrity of Science Data is significantly compromised.	Same as above.	Critical	Remote
Timing Receive (FM.SDP.PST.103)	The SDP hardware responsible for ingesting data from the CSP encounters a hardware failure impacting the data ingest island.	Without the capacity to buffer data sent by the CSP, an ingest failure at the data island level results in the loss of scan data for all beams.	Pulsar timing analysis not possible, all science data lost.	Operational reliability and efficiency are degraded. No science possible.	Attempt to reroute the data received from CSP to available correctly functioning hardware resources. The mitigation strategies from above also apply here.	Catastrophic	Extremely unlikely
QA Commands / Parameters (FM.SDP.PST.104)	The hardware executing the code that checks the correctness and validity of commands/parameters fails.	Without valid commands or parameters the pipeline must enter default mode which leads to sub-optimal processing.	Pulsar timing analysis less effective.	Efficiency degraded, minor impact on science outputs.	Operate in default mode, thereby ensuring the science data is still processed and preserved in the appropriate data archive. The data must be flagged to show it has been subjected to default mode processing.	Marginal	Remote
Remove RFI (FM.SDP.PST.105)	The hardware executing the RFI mitigation code fails.	The signal-to-noise ratio of the detected pulse will be lower without RFI mitigation.	Pulsar timing analysis less effective.	Minor impact on science outputs.	Add a flag to the data making it clear that RFI mitigation is yet to be performed, and proceed to the next step so that pipeline processing does not halt and no data lost.	Marginal	Remote
Calibrate (FM.SDP.PST.106)	The hardware executing the calibration code fails.	The signal-to-noise ratio of the detected pulse will be lower without calibration.	Pulsar timing analysis less effective.	Minor impact on science outputs.	Add a flag to the data making it clear that calibration is yet to be performed, and proceed to the next step so that pipeline processing does not halt and no data lost.	Marginal	Remote

Table 5: Hardware induced failure modes 7-11.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Average (FM.SDP.PST.107)	The hardware executing the code responsible for producing averaged data products fails.	Inability to produce intermediate output data products.	Pulsar timing analysis unaffected. Data products useful for post-processing analysis lost.	No impact on science outputs so long as primary data product is stored. Intermediate data products can be recreated via post-processing.	Add a flag to the data making it clear that averaging is yet to be performed, and proceed to the next step so that pipeline processing does not halt and no data lost.	Marginal	Remote
Archive Average Products (FM.SDP.PST.108)	The hardware executing the code that archives multiple intermediate averaged data products, and the data cube, fails.	Storage of primary and averaged data products fails.	Pulsar timing pipeline fails to persist primary science data.	Catastrophic impact on science outputs.	It is imperative that the primary data product of the timing pipeline, the data cube, is persisted. Thus this step must be re-run upon failure until the primary data product at a minimum is stored. This may hold up processing, thus may require the buffering of data from a any subsequent scans.	Critical	Remote
Determine TOAs (FM.SDP.PST.109)	The hardware executing the code that determines pulse TOAs fails.	Pulse arrival times cannot be computed.	Pulsar timing pipeline cannot measure pulse arrival times, compute residuals, and update timing models. Timing pipeline also fails to trigger alerts for profile changes of scientific interest.	Minor impact on science outputs. TOAs can be computed via post-processing if necessary.	Add a flag to the data making it clear that the TOAs could not be determined. Proceed to archive the data so that pipeline processing does not halt and no data lost.	Marginal	Remote
Archive TOAs (FM.SDP.PST.110)	The hardware executing the code that sends the computed TOAs to the archive fails.	Failure to store TOAs.	Pulsar timing pipeline fails to archive useful science data.	Minor impact on science outputs. TOAs can be computed via post-processing if necessary.	Continue retrying to archive the TOAs until some timeout period TBD has elapsed. If the TOAs cannot be archived, add a flag to the data indicating this, and proceed to the next step.	Marginal	Remote
Generate Residuals (FM.SDP.PST.111)	The hardware executing the code that generates timing residuals fails.	Failure to generate timing residuals.	Pulsar timing pipeline cannot detect scientifically interesting profile changes. This prevents rapid follow-up.	Minor impact on science outputs. Residuals can be computed via post-processing if necessary.	Add a flag to the data indicating that the residuals could not be computed. Proceed to archive the data so that pipeline processing does not halt and no data lost.	Marginal	Remote

Table 6: Hardware induced failure modes 12-16.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
QA Residuals (FM.SDP.PST.112)	The hardware executing the code that evaluates the quality of the residuals fails.	Poor quality residuals propagated through pipeline.	Pulsar timing pipeline continues processing with poor residuals.	Minor impact on science outputs. Residuals can be computed via post-processing if necessary.	Proceed to the next step so that pipeline processing does not halt and no data lost. Append a flag to the data indicating that the residuals require a QA analysis.	Marginal	Remote
Update Timing Model (FM.SDP.PST.113)	The hardware executing the code that updates the timing model fails.	Timing model not updated.	Pulsar timing pipeline cannot proceed with further processing steps.	Minor impact on science outputs. Timing model can be updated via post-processing if necessary.	Add a flag to the data making it clear that the timing model has not been updated, and proceed to archive the data so that pipeline processing does not halt and no data lost.	Marginal	Remote
Archive Timing Model (FM.SDP.PST.114)	The hardware executing the code that archives the timing model fails.	Timing model not archived.	Pulsar timing pipeline cannot carry out its primary purpose, to automatically update timing models.	Minor impact on science outputs. Timing model can be recomputed via post-processing if necessary.	Continue retrying to archive the timing model until some time-out period TBD has elapsed. If model not archived, add a flag to the data indicating this, and proceed to the data archival step.	Marginal	Remote
Evaluate Model Changes (FM.SDP.PST.115)	The hardware executing the code that evaluates changes to the timing model fails.	Inability to detect significant profile changes.	Pulsar timing pipeline cannot detect scientifically significant pulse profile changes (e.g. glitches or mode changes).	Minor to marginal impact on science outputs. Failure to evaluate prevents rapid follow-up. Data can be post-processed allowing belated evaluation.	Add a flag to the data making it clear the model has not been evaluated for change, and proceed to the data archival step so that pipeline processing does not halt and no data lost.	Marginal	Remote
Generate Alert (FM.SDP.PST.116)	The hardware executing the code that generates alerts fails.	Alerts not generated.	Pulsar timing pipeline cannot alert TM or the community to scientifically interesting events.	Minor to marginal impact on science outputs.	Add a flag to the data making it clear that the data requires follow-up analysis. Continue to attempt to generate an alert until some time-out period TBD has elapsed.	Marginal	Remote
All archiving functions (FM.SDP.PST.117)	The hardware archiving pulsar timing data (data cubes, residuals, TOAs, metadata or timing models) fails.	Science data not persisted.	Pulsar timing pipeline completes processing however science data is lost.	Marginal to Critical impact on science outputs.	If archiving fails due to a hardware error, causing data loss, the observation must be rescheduled and repeated	Marginal to Critical	Remote

5.2 Control & Communication Failures

Control failures can occur in a variety of ways. For example,

- control can be lost at the node level, due to the failure of a node management daemon or controlling SDP process.
- control can be lost at the rack or compute island level, similarly to above. This could be caused, for example, via a Top of Rack (TOR) switch failure.
- control can be lost/degraded due to a failure of the SDP management system. This can be caused by either software or hardware failures/errors. Whilst a connection to the management system will likely always be available due to the network topology used, bandwidth could be reduced.
- control can be lost due to a problem with the telescope manager, or the LMC. Note the LMC is known as the execution control system [RD9] (see section 2.1.1 in the external document) in SDP.
- control can fail due to communication errors. This could be caused by, for example, the failure of networking hardware, a network security intrusion, or the corruption of network traffic due to software problems (e.g. in firmware).
- control can fail due to use of inappropriate commands, and/or human error.

While there are many possible control failure scenarios, we consider only high level failures for brevity.

Clearly communication failures can cause many of the control issues outline above. However communication problems can also affect SDP processing, and these possibilities are considered separately. Communication failures occur due to,

- the corruption of data packets.
- networking hardware failures, or hardware failures at the node level (e.g. at the NICs).
- software errors in processing components which corrupt or invalidate communication.
- incompatible communication protocols or data types.

A number of failure modes related to control and communications are listed in Tables 7, through to Table 13 below. For simplicity only scenarios where inherent redundancy fails are presented (i.e. a worst case scenario).

Table 7: Control and Communication failure modes 1-6.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
ALL (FM.SDP.PST.201)	Control of a timing pipeline component is temporarily lost.	Timing pipeline component cannot be controlled or monitored externally.	Failure to correctly control and monitor pulsar timing processing.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised if processing conducted incorrectly.	Allow all timing pipeline components to operate autonomously in either a default or a standard mode. Attempt to confirm/re-establish control after the completion of each scan. Raise an alarm.	Minor	Remote
ALL (FM.SDP.PST.202)	Control of a timing pipeline component is lost for a period of time that exceeds a scan length.	Timing pipeline component cannot be controlled or monitored externally.	Failure to correctly control and monitor the timing processing.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised if processing conducted incorrectly.	Complete processing of data obtained during the pervious / current scan so long as commands are valid, raise an alarm, then await instruction from TM.	Minor	Remote
ALL (FM.SDP.PST.203)	Control parameters given to a timing pipeline component are incorrectly formatted or invalid.	Timing pipeline component incorrectly processes data.	Timing pipeline component cannot correctly process the data ingested from CSP causing data loss / sub-optimal processing.	Operational reliability and efficiency are degraded. Integrity of science data compromised.	Automatically detect incorrect parameters and autonomously enter default mode to prevent the loss of science data. Raise an alarm.	Minor	Remote
ALL (FM.SDP.PST.204)	Control commands given to the timing pipeline component are invalid or incorrectly formatted.	Timing pipeline component incorrectly processes data.	Timing pipeline component cannot correctly process the data ingested from CSP causing data loss / sub-optimal processing.	Operational reliability and efficiency are degraded. Integrity of science data compromised.	Automatically detect incorrect commands and autonomously enter default mode to prevent the loss of science data. Raise an alarm.	Minor	Remote
ALL (FM.SDP.PST.205)	No monitor or control signals transmitted or received from outside of the SDP.	Timing pipeline component cannot be controlled or monitored externally.	Failure to correctly control and monitor the timing processing.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised if processing conducted incorrectly.	Redundant software monitor / control network. Allow timing pipeline to operate autonomously in default mode in the event of control failure. Decouple control and monitoring within the Execution Control Component.	Minor	Remote
ALL (FM.SDP.PST.206)	No monitor or control signals transmitted or received temporarily inside of the SDP.	Timing pipeline component cannot be controlled internally.	Failure to correctly control and monitor the timing processing.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised if processing conducted incorrectly.	Redundant software monitor/-control network. Allow timing pipeline to operate autonomously in default mode in the event of control failure. Decouple control and monitoring within the Execution Control Component.	Minor	Remote

Table 8: Control and Communication failure modes 7-14.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
ALL (FM.SDP.PST.207)	No monitor or control signals transmitted or received temporarily inside of the SDP, for a period of time that exceeds a scan length.	Timing pipeline component cannot be controlled internally.	Failure to correctly control and monitor the timing processing.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised if processing conducted incorrectly.	Redundant software monitor/-control network. Complete processing of data obtained during the previous / current scan so long as commands are valid, raise an alarm, then await instruction from TM.	Minor	Remote
ALL (FM.SDP.PST.208)	Missing or corrupt monitor and control packets.	Unable to reliably monitor or control pipeline components.	Failure to correctly control and monitor the timing processing.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised if processing conducted incorrectly.	Allow timing pipeline to operate autonomously in default mode in the event of control failure.	Significant	Remote
ALL (FM.SDP.PST.209)	Routing and transmission of data within SDP fails due to missing or corrupt data packets.	Data not transmitted.	Pulsar timing analysis not possible.	Operational reliability and efficiency are degraded. All science data lost.	Resilience of routing. Allow timing pipeline to operating autonomously in default mode in the event communications failure that prioritizes saving the science data.	Significant	Remote
ALL (FM.SDP.PST.210)	Routing and transmission of data within SDP temporarily fails due to network errors or failures.	Data not transmitted.	Pulsar timing analysis not possible.	Operational reliability and efficiency are degraded. All science data lost.	Redundant data network. Resilience of routing.	Significant	Remote
ALL (FM.SDP.PST.211)	Routing and transmission of data within SDP fails due to network errors or failures, for a period of time that exceeds a scan length.	Data not transmitted.	Pulsar timing analysis not possible.	Operational reliability and efficiency are degraded. All science data lost.	Redundant data network. Resilience of routing.	Catastrophic	Extremely unlikely
ALL (FM.SDP.PST.212)	Compound routing / communication errors occurring at different locations within SDP	Data not transmitted.	Pulsar timing analysis not possible.	Operational reliability and efficiency are degraded. All science data lost.	Redundant data network. Resilience of routing. Cease processing and await TM instruction.	Catastrophic	Extremely unlikely
Timing Receive (FM.SDP.PST.213)	Control parameters sent to the timing receive component are corrupted via packet loss or some other communication error.	Timing receive incorrectly processes received data.	Timing receive cannot correctly ingest the data from CSP causing data loss.	Operational reliability and efficiency are degraded. Integrity of science data compromised.	Automatically detect incorrect parameters and autonomously enter default mode to prevent the loss of science data.	Minor	Occasional

Table 9: Control and Communication failure modes 14-19.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Timing Receive (FM.SDP.PST.214)	Routing and transmission of data from the CSP fails due to too many missing or corrupt data packets.	No pulsar timing data received.	Pulsar timing analysis not possible.	Operational reliability and efficiency are degraded. All science data lost.	Resilience of routing. The capacity to request that data be resent.	Catastrophic	Remote
Timing Receive (FM.SDP.PST.215)	Routing and transmission of data from the CSP temporarily fails due to network communication failures.	No pulsar timing data received.	Pulsar timing analysis not possible.	Operational reliability and efficiency are degraded. All science data lost.	Re-establish connectivity, and if possible request scan data be resent from CSP.	Catastrophic	Remote
Timing Receive (FM.SDP.PST.216)	Data received from the CSP is marginally corrupted via packet loss or some other communication error.	Timing receive processes partly corrupted data.	Pulsar timing analysis less effective.	Science data loses some of its utility.	Monitor proportion of data subject to corruption. Continue to function normally so long as less than 20% TBC of the data is corrupted. If more than 20% TBC is corrupted raise an alarm, but continue to function and annotate the processed data with a flag indicating that its utility is significantly degraded.	Marginal	Occasional
Timing Receive (FM.SDP.PST.217)	Timing receive temporarily loses connectivity with downstream SDP components.	Timing receive cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Scientific output not produced.	Send the science data to the preservation system without processing to prevent data loss. Flag the data as requiring follow-up post-processing. Generate an alert.	Marginal	Remote
Timing Receive (FM.SDP.PST.218)	Timing receive loses all connectivity with downstream SDP components for a period of time longer than a scan duration.	Timing receive cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Scientific output not produced.	Resilience of routing.	Catastrophic	Extremely unlikely
Timing Receive / Ingest (FM.SDP.PST.219)	Failure to ingest received data in a timely fashion, causing a data backlog which cannot be cached.	Data does not enter the pipeline quickly enough to complete timing processing in the allotted time.	Pulsar timing analysis incomplete.	Scientific outputs degraded. Science data loses some of its utility, some data loss.	Resilience of routing, automatic load balancing to prevent resource contention and processing delays.	Marginal	Remote

Table 10: Control and Communication failure modes 20-23.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Timing Receive / Ingest (FM.SDP.PST.220)	Sub-integration data impacted by packet loss when using FTP (as data sent 1 sub-int at a time).	Timing receive processes partly corrupted data. Mitigation strategy incurs computational overhead.	Reduced effectiveness of pulsar timing analysis.	Minor degradation to science outputs.	Request that data be resent. If resend impossible, add a zeroed sub-int in place of the corrupted sub-int. Update cumulative tracking of lost sub-ints and sub-int samples. If cumulative data loss more than 20% TBC then too much signal has been lost and an alarm must be raised. Tag the data so the proportion of lost sub-ints is recorded.	Scan dependent. Fractional loss is important. Severity ranges from minor to critical due to cumulative effects.	Occasional
Remove RFI (FM.SDP.PST.221)	Remove RFI function temporarily loses connectivity with downstream SDP components.	Remove RFI function cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Scientific output degraded.	Retry sending the data until some time-out period TBD has elapsed. If retry fails, send the science data to the preservation system without processing to prevent data loss. Flag the data as requiring follow-up post-processing. Generate an alert.	Marginal	Remote
Calibrate (FM.SDP.PST.222)	Calibrate function temporarily loses connectivity with downstream SDP components.	Calibrate function cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Scientific output degraded.	Retry sending the data until some time-out period TBD has elapsed. If retry fails, send the science data to the preservation system without processing to prevent data loss. Flag the data as requiring follow-up post-processing. Generate an alert.	Marginal	Remote
Archive Average Products (FM.SDP.PST.223)	Average function temporarily loses connectivity with downstream SDP components.	Average function cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Scientific output not produced.	Retry sending the data until some time-out period TBD has elapsed. If retry fails, send the science data to the preservation system without processing to prevent data loss. Flag the data as requiring follow-up post-processing. Generate an alert.	Marginal	Remote

Table 11: Control and Communication failure modes 24-28.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Archive Average Products (FM.SDP.PST.224)	Connectivity with the preservation system is temporarily lost, preventing storage of averaged data products and the primary data cube.	Storage of primary and averaged data products fails.	Pulsar timing pipeline fails to persist primary science data.	Potential for critical impact on science outputs.	It is imperative for the primary data product of the timing pipeline, the data cube, to be persisted. Thus this step must be re-run upon failure until the primary data product at a minimum is stored. Or until some time-out period TBD has elapsed. Generate an alert. If the data is retained in a buffer and not discarded until science outputs are persisted, then the severity is reduced to marginal.	Marginal to Critical	Remote
Archive Average Products (FM.SDP.PST.225)	Archive Average Products function temporarily loses connectivity with downstream SDP components.	Archive Average Products function cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Some scientific output not produced.	Generate an alert, and prepare for next scan (no further processing possible). Flag the data for follow-up post processing.	Minor	Remote
Determine TOAs (FM.SDP.PST.226)	Determine TOAs function temporarily loses connectivity with downstream SDP components.	Determine TOAs function cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Some scientific output not produced.	Retry sending the data until some time-out period TBD has elapsed. Generate an alert if data is not sent, and prepare for the next scan (no further processing possible). Flag the data for follow-up post processing.	Minor	Remote
Archive TOAs (FM.SDP.PST.227)	Connectivity with the preservation system is temporarily lost, preventing the storage of TOAs.	Failure to store TOAs.	Pulsar timing pipeline fails to archive useful science data.	Minor impact on science outputs. TOAs can be computed via post-processing if necessary.	Continue to attempt to archive the TOAs until some time-out period TBD has elapsed. If archiving fails, add a flag to the data making it clear that the TOAs have not been archived. Proceed to the next step so that pipeline processing does not halt and no data lost.	Marginal	Remote
Archive TOAs (FM.SDP.PST.228)	Archive TOAs function temporarily loses connectivity with downstream SDP components.	Archive TOAs function cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Some scientific output not produced.	Retry sending the data until some time-out period TBD has elapsed. Generate an alert if data is not sent. Flag the data for follow-up post processing.	Minor	Remote

Table 12: Control and Communication failure modes 29-33.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Generate Residuals (FM.SDP.PST.229)	Generate Residuals function temporarily loses connectivity with downstream SDP components.	Generate Residuals function cannot pass data through the timing pipeline.	Pulsar timing analysis not possible.	Some scientific output not produced.	Retry sending the data until some time-out period TBD has elapsed. If the data is not sent, generate an alert. Then prepare for the next scan (no further processing possible). Flag the data for follow-up post processing.	Minor	Remote
Send Residuals to QA System (FM.SDP.PST.230)	Send Residuals to QA System function temporarily loses connectivity with downstream SDP components.	Send Residuals to QA System function cannot pass data through the timing pipeline.	Pulsar timing analysis quality reduced.	Quality of science output affected.	Retry sending the data until some time-out period TBD has elapsed. Generate an alert, and flag the data for residual QA, and move to the next processing step.	Minor	Remote
Update Timing Model(FM.SDP.PST.231)	Timing model for the pulsar being observed cannot be obtained externally.	Timing model not updated.	Pulsar timing pipeline cannot proceed with further processing steps.	Minor impact on science outputs. Timing model can be updated via post-processing if necessary.	Continue to attempt to obtain the timing model until some time-out period TBD has elapsed. If unavailable on retry, add a flag to the data indicating this. Proceed to the next step so that pipeline processing does not halt and no data lost.	Marginal	Remote
Evaluate Model Changes (FM.SDP.PST.232)	Evaluate Model Changes function temporarily loses connectivity with downstream SDP components.	Evaluate Model Changes function cannot pass data through the timing pipeline.	Cannot generate alerts based of changes in a timing profile.	Quality of science output affected.	Generate an alert, and flag the data for model change analysis post-processing. Then proceed to archive the timing model.	Minor	Remote
Archive Timing Model (FM.SDP.PST.233)	Connectivity with the preservation system is temporarily lost, preventing storage of the updated timing model.	Timing model not sent to the archive/preservation system.	Timing model not archived. Pipeline fails to automatically update timing models.	Minor impact on science outputs. Timing model can be recomputed via post-processing if necessary.	Retry sending the data until some timeout period TBD has elapsed. If the data is not sent, raise an alarm. Add a flag to the data making it clear the timing model has not been persisted. Proceed to the next step so that pipeline processing does not halt and no data lost.	Marginal	Remote

Table 13: Control and Communication failure modes 34-36.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Update Timing Model (FM.SDP.PST.234)	Update Timing Model function temporarily loses connectivity with downstream SDP components.	Update Timing Model function cannot pass data through the timing pipeline.	Timing model not updated.	Automatic update of timing models fails.	Generate an alert, and flag the data for follow-up post processing.	Minor	Remote
Generate Alert (FM.SDP.PST.235)	Connectivity with the alert system is temporarily lost, preventing rapid follow-up.	Alerts not generated.	Pulsar timing pipeline cannot alert TM or the research community to scientifically interesting events.	Minor to marginal impact on science outputs.	Add a flag to the data making it clear that the data requires follow-up analysis. Continue to attempt to generate an alert until some time-out period TBD has elapsed.	Marginal	Remote
ALL - Metadata Acquisition (FM.SDP.PST.236)	Connectivity with the system/s responsible for managing and supplying metadata is temporarily lost. This impacts the acquisition of sky models, RFI masks, calibration strategies, pulsar ephemerides, Standard Profiles and timing models	Data required for processing not available, causing processing steps to be missed.	Pulsar timing pipeline unable to run correctly.	Minor to marginal impact on science outputs.	Retry obtaining the required metadata until some time-out period TBD has elapsed. If metadata still unavailable, generate an alert. Add a flag to the data making it clear that the data requires follow-up analysis. Proceed to the next processing step where possible in default mode.	Marginal	Remote

5.3 Data Failures

Data failures arise when data is incorrectly formatted, contains invalid values, or is not provided when expected. Formatting and validity issues typically arise through software errors and incorrectly implemented interfaces. It is also possible for such errors to occur due to communication issues (e.g. packet loss), or memory problems (e.g. bit flips) that can cause data corruption.

Data problems can also arise when using external databases. It is possible for data requested of an external resource to become corrupted during transfer, or data mismanagement. As the pulsar timing pipeline requires external data to function (e.g. pulsar ephemerides), such errors are plausible.

A number of failure modes related to data are listed in Tables 14, through to Table 16.

Table 14: Data failure modes 1-6.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Timing Receive / Ingest (FM.SDP.PST.301)	Sub-integration data incorrectly formatted / contains invalid values.	Timing receive processes partly corrupted or incorrectly formatted data. Mitigation strategy incurs computational overhead.	Reduced effectiveness of pulsar timing analysis.	Minor degradation to science outputs.	Add a zeroed sub-int in place of incorrectly formatted or invalid sub-integration (or sub-int data point). Update cumulative tracking of lost sub-ints and sub-int samples. If cumulative data loss more than 20% TBC then too much signal has been lost and an alarm must be raised. Tag the data so the proportion of lost sub-ints is recorded.	Scan dependent. Fractional loss is important. Severity ranges from minor to critical due to cumulative effects.	Remote
Remove RFI (FM.SDP.PST.302)	No RFI mask provided.	Cannot remove/mitigate RFI. The signal-to-noise ratio of the detected pulse will be lowered.	Pulsar timing analysis less effective.	Minor to Marginal impact on science outputs.	Add a flag to the data making it clear that RFI mitigation is yet to be performed, and proceed to the next processing step so that pipeline processing does not halt and no data lost.	Marginal	Extremely Unlikely
Remove RFI (FM.SDP.PST.303)	Invalid / corrupt RFI mask provided to the RFI mitigation component.	Cannot remove/mitigate RFI. The signal-to-noise ratio of the detected pulse will be lowered.	Pulsar timing analysis less effective.	Minor to Marginal impact on science outputs.	Same as FM.SDP.PST.302.	Marginal	Remote
Remove RFI (FM.SDP.PST.304)	Inappropriate RFI mask provided to the RFI mitigation component.	The signal-to-noise ratio of the detected pulse will be lower without RFI mitigation.	Pulsar timing analysis less effective.	Minor to Marginal impact on science outputs.	Undo the mitigation step and Add a flag to the data making it clear that RFI mitigation is yet to be performed. Must also explain that the applied mask failed to increase the signal-to-noise ratio.	Minor	Occasional
Calibrate (FM.SDP.PST.305)	No calibration solution provided.	The signal-to-noise ratio of the detected pulse will be lower without calibration.	Pulsar timing analysis less effective.	Minor impact on science outputs.	Add a flag to the data making it clear that calibration is yet to be performed, and proceed to the next processing step so that pipeline processing does not halt and no data lost.	Marginal	Remote
Calibrate (FM.SDP.PST.306)	Invalid / corrupt calibration solution provided.	The signal-to-noise ratio of the detected pulse will be lower without calibration.	Pulsar timing analysis less effective.	Minor impact on science outputs.	Same as FM.SDP.PST.305.	Marginal	Remote

Table 15: Data failure modes 7-11.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Calibrate (FM.SDP.PST.307)	Inappropriate calibration solution provided.	The signal-to-noise ratio of the detected pulse will be lower without calibration.	Pulsar timing analysis less effective.	Minor impact on science outputs.	Undo the calibration step and add a flag to the data making it clear that calibration is yet to be performed. Must also explain that the applied strategy failed to increase the signal-to-noise ratio.	Minor	Occasional
Average (FM.SDP.PST.308)	No specifications provided for the required averaged data products.	Inability to produce intermediate output data products.	Pulsar timing analysis unaffected. Only data products useful for post-processing analysis are lost.	No impact on science outputs so long as the primary data product is stored. Intermediate data products can be recreated via post-processing.	Send the primary data cube to the preservation archive, along with some default averaged data products.	Minor	Occasional
Archive Average Products (FM.SDP.PST.309)	Averaged data products incorrectly formatted / contain invalid values due to software error.	Averaged data products are not persisted. Cannot send invalid or corrupted data to the preservation archive.	Pulsar timing analysis unaffected. Only data products useful for post-processing analyses are lost.	No impact on science outputs so long as the primary data product is stored. Intermediate data products can be recreated via post-processing.	Send the primary data cube to the preservation archive. Flag that average data products were invalid and need recreating. Raise an alarm.	Minor	Remote
Determine TOAs (FM.SDP.PST.310)	No standard profile provided.	No TOAs determined.	Pulsar timing analysis incomplete.	Minor to Marginal impact on science outputs.	Retry obtaining the standard profile until some time-out period TBD has elapsed. If none available, enter default mode and send the data to the preservation archive. Annotate the data and flag for reprocessing. Prepare to process the next scan (cannot proceed with timing processing without the standard profile). Raise an alarm.	Marginal	Remote
Determine TOAs (FM.SDP.PST.311)	Invalid / corrupt standard profile provided.	No TOAs determined.	Pulsar timing analysis incomplete.	Minor to Marginal impact on science outputs.	Retry obtaining the standard profile until some time-out period TBD has elapsed. If none available, enter default mode and send the data to the preservation archive. Annotate the data and flag for reprocessing. Prepare to process the next scan (cannot proceed without the standard profile). Raise an alarm.	Marginal	Remote

Table 16: Data failure modes 12-17.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
Archive TOAs (FM.SDP.PST.312)	Invalid / corrupt computed TOAs due to software errors.	Failure to store TOAs. Cannot send invalid or corrupted data to the preservation archive.	Pulsar timing pipeline fails to archive useful science data.	Minor impact on science outputs. TOAs can be computed via post-processing if necessary.	Raise an alarm, and flag the data indicating that TOAs need to be computed during post-processing.	Marginal	Remote
Generate Residuals (FM.SDP.PST.313)	Invalid / corrupt computed TOAs due to software errors.	Cannot compute residuals from invalid / corrupt TOAs.	Pulsar timing pipeline fails to compute residuals for the observed pulsar. Cannot detect scientifically interesting profile changes.	Minor impact on science outputs. TOAs can be computed via post-processing if necessary.	Raise an alarm, and flag the data indicating that TOAs and residuals need to be computed during post-processing.	Marginal	Remote
QA Residuals (FM.SDP.PST.314)	Invalid / corrupt residuals provided, unable to asses their quality.	Cannot continue processing.	Pulsar timing pipeline halts.	Minor impact on science outputs. Residuals can be computed via post-processing if necessary.	Raise an alarm, and flag the data indicating that residuals need to be computed during post-processing.	Marginal	Remote
Update Timing Model (FM.SDP.PST.315)	Invalid / corrupt residuals provided, unable to update the timing model.	Timing model not updated.	Pulsar timing pipeline cannot proceed with further processing steps.	Minor impact on science outputs. Timing model can be updated via post-processing if necessary.	Raise an alarm, and flag the data indicating that residuals need to be computed during post-processing.	Marginal	Remote
Update Timing Model / Archive Timing Model (FM.SDP.PST.316)	Invalid / corrupt timing model provided, unable to update.	Timing model not updated.	Pulsar timing pipeline cannot proceed with further processing steps.	Minor impact on science outputs. Timing model can be updated via post-processing if necessary.	Raise an alarm, and flag the data indicating that the timing model needs to be updated during post-processing.	Marginal	Remote

5.4 Software/Algorithm Failures

Software and algorithms can fail for a variety of reasons. The causes range from bugs inadvertently introduced at the software design stage, to bugs accidental coded during implementation. Aside from bugs, software can also fail when,

- non-deterministic algorithms do not complete on certain types of input data.
- software/algorithm logic is incorrectly coded preventing loops from terminating.
- numerical precision is incorrectly handled, causing sub-optimal performance or failure.
- incorrect data types are used when handling numerical data causing precision errors.
- errors in parallelism cause data to be incorrectly processed, for example, via memory access errors.
- slow runtime which causes failures at the system level (due to delay).
- similarly sub-optimal implementation, which causes failures at the system level (due to resource contention).
- security vulnerabilities are exploited by attackers.

A number of failure modes related to software/algorithms are listed in Tables 17 and Table 18.

Table 17: Software/Algorithm failure modes 1-9.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
ALL (FM.SDP.PST.401)	Function, process or application throws an arithmetic error (divide by zero, arithmetic overflow or underflow, loss of precision).	Function fails to complete execution.	Timing pipeline fails to complete an assigned task.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised.	Execution framework re-runs function / algorithm again with input data. Error report logged and fed to software development team for investigation.	Critical	Extremely unlikely
ALL (FM.SDP.PST.402)	Function, process or application encountered a logic error (infinite loops or infinite recursion, loop counter errors, array index out of bounds exception).	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Critical	Extremely unlikely
ALL (FM.SDP.PST.403)	Function, process or application encountered a resource error (Null pointer, access violations, resource leaks, buffer overflow-use-after-free error).	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Critical	Extremely unlikely
ALL (FM.SDP.PST.404)	Function, process or application encountered a multi-threading error.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Critical	Extremely unlikely
ALL (FM.SDP.PST.405)	Function, process or application encountered an interface error.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Same as for FM.SDP.PST.401.	Critical	Extremely unlikely
ALL (FM.SDP.PST.406)	Non-deterministic data dependent function does not terminate in allotted time.	Function fails to complete execution.	Timing pipeline fails to complete an assigned task.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised.	Monitor processing progress, and force early termination if function / algorithm not converging. Tag the processed data with a note explaining how the processing was curtailed. Generate a log entry explaining how to reproduce the error mode.	Critical	Remote
ALL (FM.SDP.PST.407)	Function, process or application does not respond to commands in a timely manner.	Components can't be configured correctly.	Timing pipeline can complete execution, but possibly with sub-optimal configuration, e.g. default mode.	Integrity of science data could be compromised.	Re-start the function / process prior to the next scan. Generate a log entry describing the error state and steps to reproduce.	Critical	Remote
ALL (FM.SDP.PST.408)	Runtime exceeds allotted time.	Processing backlog created.	Places additional load on processing resources.	Integrity of science data could be compromised if some data cannot be processed.	If runtime begins to increase automatically load balance to provide additional resources.	Minor	Occasional

Table 18: Software/Algorithm failure modes 9-14.

Function	FM Description	Local Effect	Sub-system Effect	System Effect	Mitigation	Severity	Likelihood
ALL (FM.SDP.PST.409)	Communication time-out caused by network connectivity issues.	Inability to process data.	Timing pipeline fails to complete an assigned task.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised.	Retry obtaining the data until some time-out period TBD has elapsed. Generate an alert.	Minor	Occasional
ALL (FM.SDP.PST.410)	Function, process or application becomes unresponsive.	Inability to process data.	Timing pipeline fails to complete an assigned task.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised.	Re-start the function immediately. Generate a log entry describing the error state and steps to reproduce.	Minor	Remote
ALL (FM.SDP.PST.411)	Error checking procedures fail in the executing application or function.	Inability to process data.	Timing pipeline fails to complete an assigned task.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised.	Re-start the function immediately. Generate a log entry describing the error state and steps to reproduce.	Minor	Extremely unlikely
ALL (FM.SDP.PST.412)	Security breaches and intrusions occurring during normal execution.	Inability to process data.	Timing pipeline fails to complete an assigned task.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised.	Terminate all functions and processes and generate an alert.	Minor	Extremely unlikely
ALL (FM.SDP.PST.413)	In memory errors caused by bit flips or power surges corrupting executing code.	Inability to process data.	Timing pipeline fails to complete an assigned task.	Operational reliability and efficiency are degraded. Integrity of science data could be compromised.	Re-start the function immediately. Generate a log entry describing the error state and steps to reproduce. Generate an alert.	Minor	Extremely unlikely

6 Summary

In this document we have summarised pulsar timing pipeline failure modes at a high level of abstraction. Numerous failure types have been identified and contextualised according to number of key assumptions. Our next steps will be to improve upon this work following feedback from our SDP colleagues, and incorporate those improvements into analyses of pulsar and transient search pipeline failure modes.

A FMECA Detection methods

Table 19 through to Table 21 summarises the detection methods for each failure mode.

Table 19: Summary of the detection methods for each of the failure modes discussed in this document (Part 1).

Failure Mode Code	Detection Method
FM.SDP.PST.101	Monitor the health status of the SDP data ingest nodes, and monitor network connectivity status.
FM.SDP.PST.102	Same as for FM.SDP.PST.101.
FM.SDP.PST.103	Same as for FM.SDP.PST.101.
FM.SDP.PST.104	Monitor the health status of the SDP compute nodes, and monitor network connectivity status.
FM.SDP.PST.105	Same as for FM.SDP.PST.104.
FM.SDP.PST.106	Same as for FM.SDP.PST.104.
FM.SDP.PST.107	Same as for FM.SDP.PST.104.
FM.SDP.PST.108	Same as for FM.SDP.PST.104.
FM.SDP.PST.109	Same as for FM.SDP.PST.104.
FM.SDP.PST.110	Same as for FM.SDP.PST.104.
FM.SDP.PST.111	Same as for FM.SDP.PST.104.
FM.SDP.PST.112	Same as for FM.SDP.PST.104.
FM.SDP.PST.113	Same as for FM.SDP.PST.104.
FM.SDP.PST.114	Same as for FM.SDP.PST.104.
FM.SDP.PST.115	Same as for FM.SDP.PST.104.
FM.SDP.PST.116	Same as for FM.SDP.PST.104.
FM.SDP.PST.117	Same as for FM.SDP.PST.104.
FM.SDP.PST.201	Monitor the health status of software modules, and monitor network connectivity status.
FM.SDP.PST.202	Monitor the health status of software modules, and monitor network connectivity status.
FM.SDP.PST.203	QA of control parameters sent between TM/LMC and the timing pipeline components.
FM.SDP.PST.204	QA of control commands sent between TM/LMC and the timing pipeline components.
FM.SDP.PST.205	Active monitoring of software components and the communication network between them.
FM.SDP.PST.206	Active monitoring of software components and the communication network between them.
FM.SDP.PST.207	Active monitoring of software components and the communication network between them.

Table 20: Summary of the detection methods for each of the failure modes discussed in this document (Part 2).

Failure Mode Code	Detection Method
FM.SDP.PST.208	Active monitoring of software components and the communication network between them.
FM.SDP.PST.209	Active monitoring of data processing hardware.
FM.SDP.PST.210	Active monitoring of data processing hardware.
FM.SDP.PST.211	Active monitoring of data processing hardware.
FM.SDP.PST.212	Active monitoring of data processing hardware.
FM.SDP.PST.213	QA of control parameters sent between TM/LMC and the timing pipeline component.
FM.SDP.PST.214	Active monitoring of data processing hardware.
FM.SDP.PST.215	Monitor network connectivity status.
FM.SDP.PST.216	Monitor network connectivity status and QA of received data.
FM.SDP.PST.217	Monitor network connectivity status and QA of received data.
FM.SDP.PST.217	Monitor network connectivity status and QA of received data.
FM.SDP.PST.218	Monitor network connectivity status and QA of received data.
FM.SDP.PST.219	Monitor the processing load placed upon data ingest nodes, and monitor network connectivity status.
FM.SDP.PST.220	Monitor cumulative sub-integration loss for each beam per scan.
FM.SDP.PST.221	Monitor network connectivity status and QA of received data.
FM.SDP.PST.222	Monitor network connectivity status and QA of received data.
FM.SDP.PST.223	Monitor network connectivity status and QA of received data.
FM.SDP.PST.224	Monitor network connectivity status and QA of received data.
FM.SDP.PST.225	Monitor network connectivity status and QA of received data.
FM.SDP.PST.226	Monitor network connectivity status and QA of received data.
FM.SDP.PST.227	Monitor network connectivity status and QA of received data.
FM.SDP.PST.228	Monitor network connectivity status and QA of received data.
FM.SDP.PST.229	Monitor network connectivity status and QA of received data.
FM.SDP.PST.230	Monitor network connectivity status and QA of received data.
FM.SDP.PST.231	Monitor network connectivity status and QA of received data.
FM.SDP.PST.232	Monitor network connectivity status and QA of received data.
FM.SDP.PST.233	Monitor network connectivity status and QA of received data.
FM.SDP.PST.234	Monitor network connectivity status and QA of received data.
FM.SDP.PST.235	Monitor network connectivity status and QA of received data.
FM.SDP.PST.236	Monitor network connectivity status and QA of received data.

Table 21: Summary of the detection methods for each of the failure modes discussed in this document (Part 3).

Failure Mode Code	Detection Method
FM.SDP.PST.301	QA the data received to ensure it is formatted correctly and contains valid data values.
FM.SDP.PST.302	Check that the RFI mask is valid.
FM.SDP.PST.303	Check that the RFI mask is valid.
FM.SDP.PST.304	Check the signal-to-noise ratio of the detected pulse increases post RFI mitigation.
FM.SDP.PST.305	Check for valid calibration strategy.
FM.SDP.PST.306	Check for valid calibration strategy.
FM.SDP.PST.307	Check the signal-to-noise ratio of the detected pulse increases post calibration.
FM.SDP.PST.308	Check for valid configuration.
FM.SDP.PST.309	QA the format and values of the averaged data products.
FM.SDP.PST.310	QA the standard profile.
FM.SDP.PST.311	QA the standard profile.
FM.SDP.PST.312	QA the computed TOAs.
FM.SDP.PST.313	QA the computed TOAs.
FM.SDP.PST.314	QA the residuals.
FM.SDP.PST.315	QA the residuals.
FM.SDP.PST.316	QA the residuals.
FM.SDP.PST.401	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.402	Same as for FM.SDP.PST.401.
FM.SDP.PST.403	Same as for FM.SDP.PST.401.
FM.SDP.PST.404	Same as for FM.SDP.PST.401.
FM.SDP.PST.405	Same as for FM.SDP.PST.401.
FM.SDP.PST.406	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.406	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.407	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.408	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.409	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.410	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.411	Process monitoring at the operating system / execution framework level.
FM.SDP.PST.412	Process monitoring at the operating system / execution framework level.

B FMECA Results

Table 22 through to Table 24 summarises the results of our analysis.

Table 22: Summary of the criticality scores for each of the failure modes discussed in this document (Part 1).

Failure Mode Code	Severity	Probability	Score
FM.SDP.PST.101	Minor	Occasional	3
FM.SDP.PST.102	Critical	Remote	8
FM.SDP.PST.103	Catastrophic	Extremely unlikely	5
FM.SDP.PST.104	Marginal	Remote	4
FM.SDP.PST.105	Marginal	Remote	4
FM.SDP.PST.106	Marginal	Remote	4
FM.SDP.PST.107	Marginal	Remote	4
FM.SDP.PST.108	Critical	Remote	8
FM.SDP.PST.109	Marginal	Remote	4
FM.SDP.PST.110	Marginal	Remote	4
FM.SDP.PST.111	Marginal	Remote	4
FM.SDP.PST.112	Marginal	Remote	4
FM.SDP.PST.113	Marginal	Remote	4
FM.SDP.PST.114	Marginal	Remote	4
FM.SDP.PST.115	Marginal	Remote	4
FM.SDP.PST.116	Marginal	Remote	4
FM.SDP.PST.117	Marginal to Critical	Remote	4 to 8
FM.SDP.PST.201	Minor	Remote	2
FM.SDP.PST.202	Minor	Remote	2
FM.SDP.PST.203	Minor	Remote	2
FM.SDP.PST.204	Minor	Remote	2
FM.SDP.PST.205	Minor	Remote	2
FM.SDP.PST.206	Minor	Remote	2
FM.SDP.PST.207	Minor	Remote	2
FM.SDP.PST.208	Significant	Remote	6
FM.SDP.PST.209	Significant	Remote	6
FM.SDP.PST.210	Significant	Remote	6
FM.SDP.PST.211	Catastrophic	Extremely unlikely	5
FM.SDP.PST.212	Catastrophic	Extremely unlikely	5
FM.SDP.PST.213	Minor	Occasional	3
FM.SDP.PST.214	Catastrophic	Remote	6

Table 23: Summary of the criticality scores for each of the failure modes discussed in this document (Part 2).

Failure Mode Code	Severity	Probability	Score
FM.SDP.PST.215	Catastrophic	Remote	10
FM.SDP.PST.216	Marginal	Occasional	6
FM.SDP.PST.217	Marginal	Remote	4
FM.SDP.PST.218	Catastrophic	Extremely unlikely	4
FM.SDP.PST.219	Marginal	Remote	4
FM.SDP.PST.220	Scan dependent. Fractional loss is important. Severity ranges from minor to critical due to cumulative effects.	Occasional	2 to 8
FM.SDP.PST.221	Marginal	Remote	4
FM.SDP.PST.222	Marginal	Remote	4
FM.SDP.PST.223	Marginal	Remote	4
FM.SDP.PST.224	Marginal to Critical	Remote	4 to 8
FM.SDP.PST.225	Minor	Remote	2
FM.SDP.PST.226	Minor	Remote	2
FM.SDP.PST.227	Marginal	Remote	4
FM.SDP.PST.228	Minor	Remote	2
FM.SDP.PST.229	Minor	Remote	2
FM.SDP.PST.230	Minor	Remote	2
FM.SDP.PST.231	Marginal	Remote	4
FM.SDP.PST.232	Minor	Remote	2
FM.SDP.PST.233	Marginal	Remote	4
FM.SDP.PST.234	Minor	Remote	2
FM.SDP.PST.235	Marginal	Remote	4
FM.SDP.PST.236	Marginal	Remote	4
FM.SDP.PST.315	Marginal	Remote	4
FM.SDP.PST.316	Marginal	Remote	4
FM.SDP.PST.301	Scan dependent. Fractional loss is important. Severity ranges from minor to critical due to cumulative effects.	Remote	2 to 8
FM.SDP.PST.302	Marginal	Extremely Unlikely	4
FM.SDP.PST.303	Marginal	Remote	4
FM.SDP.PST.304	Minor	Occasional	4
FM.SDP.PST.305	Marginal	Remote	4
FM.SDP.PST.306	Marginal	Remote	4
FM.SDP.PST.307	Minor	Occasional	3
FM.SDP.PST.308	Minor	Occasional	4
FM.SDP.PST.309	Minor	Remote	4
FM.SDP.PST.310	Marginal	Remote	4
FM.SDP.PST.311	Marginal	Remote	4
FM.SDP.PST.312	Marginal	Remote	4
FM.SDP.PST.313	Marginal	Remote	4

Table 24: Summary of the criticality scores for each of the failure modes discussed in this document (Part 3).

Failure Mode Code	Severity	Probability	Score
FM.SDP.PST.314	Marginal	Remote	4
FM.SDP.PST.315	Marginal	Remote	4
FM.SDP.PST.316	Marginal	Remote	4
FM.SDP.PST.401	Critical	Extremely unlikely	4
FM.SDP.PST.402	Critical	Extremely unlikely	4
FM.SDP.PST.403	Critical	Extremely unlikely	4
FM.SDP.PST.404	Critical	Extremely unlikely	4
FM.SDP.PST.405	Critical	Extremely unlikely	4
FM.SDP.PST.406	Critical	Remote	8
FM.SDP.PST.406	Critical	Remote	8
FM.SDP.PST.407	Minor	Occasional	3
FM.SDP.PST.408	Minor	Occasional	3
FM.SDP.PST.409	Minor	Remote	2
FM.SDP.PST.410	Minor	Extremely unlikely	1
FM.SDP.PST.411	Minor	Extremely unlikely	1
FM.SDP.PST.412	Minor	Extremely unlikely	1

C Applicable Requirements

We currently do not have access to Innoslate, thus these requirements may not be up-to-date.

Table 25: Level 2 SDP requirements relevant to the failure mode analysis.

Requirement ID	Name	Description
SDP_REQ-30	Graceful degradation	The failure of a single component should not cause the SDP to become unavailable.
SDP_REQ-33	Flagging control	The SDP shall flag data according to a pre-selected RFI Mask.
SDP_REQ-52	Failsafe	The SDP shall actively ensure that internal failures do not result in a hazardous situation to the systems and personnel with which it interfaces.
SDP_REQ-133	Pulsar Search Post Processing	SDP shall be capable of operating in a pulsar search mode, concurrently with continuum imaging mode, single pulse transient search mode and pulsar timing mode, within the same subarray.
SDP_REQ-276	Data Product Provenance	The SDP shall create and maintain provenance links between science data products and observing projects and proposals.

SDP_REQ-281	Protection against data loss	The SDP shall protect the preserved science data products against data loss and malicious or accidental modification.
SDP_REQ-285	Accessibility	The SDP shall enable per user access to SDP resources (hardware and software) using the Authentication and Authorisation facilities provided by the SKA (as per EN 50600-2-5. Data centre facilities and infrastructures. Part 2-5. Security systems).
SDP_REQ-450	SDP standard pipeline products	The SDP shall produce processing logs and quality assessment logs for all pipelines. These should be traceable to the originating Schedule Blocks.
SDP_REQ-470	Receive Data	The SDP shall receive the observed data from CSP in compliance with the SDP-CSP ICD 100-000000-002 and 300-000000-002.
SDP_REQ-472	Handle Missing Data	The SDP shall be capable of handling missing data packets coming from CSP in such a way that it minimises the scientific impact of the lost data.
SDP_REQ-476	Flag RFI	The SDP shall be capable of automatically flagging known and unknown RFI using algorithms as applied in the AOFlagger.
SDP_REQ-477	Excise RFI	The SDP shall be capable of automatically excising known and unknown RFI.
SDP_REQ-478	Detect RFI	The SDP shall be capable of detecting data that is corrupted by RFI.
SDP_REQ-479	Remove Sources	The SDP shall be capable of removing strong sources at the highest time and frequency resolution.
SDP_REQ-480	Integrate Data	The SDP shall be capable of integrating data in time and/or frequency.
SDP_REQ-524	Pulsar Timing Input	SDP shall be capable of receiving pulsar timing data and dynamic spectrum data in accordance with the SDP-CSP Interface Control Document (100-000000-002 and 300-000000-002).
SDP_REQ-527	Pulsar Search Data Input	The SDP shall be capable of receiving pulsar periodicity search data in accordance with the SDP-CSP Interface Control Document (100-000000-002 and 300-000000-002).

SDP_REQ-529	Pulsar Timing Precision	When provided with a suitable template, signal-to-noise and pulsar parameters, SDP shall be able to measure the arrival time of a pulse with a precision of 5ns.
SDP_REQ-530	Pulsar Timing ToA Determination	SDP shall be capable of determining the time of arrival of a pulse from pulsar timing data.
SDP_REQ-532	Single pulse Transient Post Processing	SDP shall be capable of operating in a single pulse transient search mode, concurrently with continuum imaging mode and pulsar search mode and pulsar timing mode, within the same subarray.
SDP_REQ-534	Pulsar Timing Data Preparation	SDP shall be capable of performing data pre-processing (adding the sub-integrations from each pulsar together into one data file) on pulsar timing data.
SDP_REQ-539	Non-imaging Transient Input	SDP shall be capable of receiving single pulse transient search data in accordance with the SDP-CSP Interface Control Document (100-000000-002 and 300-000000-002).
SDP_REQ-542	Pulsar Timing Error Estimation	SDP shall be able to estimate the uncertainty in the arrival time of a pulse to better than 5%.
SDP_REQ-543	Pulsar Timing Systematic Error	SDP shall not add more than 5ns systematic error in the time-of-arrival determination.
SDP_REQ-544	Single pulse Transient Alerts	SDP shall provide preliminary alerts for the detection of fast (single pulse) transient events within 10s of the data containing that event arriving at the SDP.
SDP_REQ-546	Single pulse Transient Search Output	SDP shall output a single ranked list of single pulse transient candidates (with durations greater 50 μsec) from each observation.
SDP_REQ-558	Pulsar Search Output	SDP shall output a single ranked list of pulsar periodicity candidates from each observation.
SDP_REQ-565	Pulsar Timing Model Fitting	SDP shall be capable of fitting a pulsar timing model to pulsar times of arrival.
SDP_REQ-640	Single Pulse data preparation performance	While receiving single pulse transient search data the SDP shall prepare the data for processing within 100 milliseconds.

SDP_REQ-641	Transient Buffer Receive Mid	The SKA1_MID SDP shall start recording Transient Buffer data no later than 60 seconds from the time that the highest frequency component of a transient signal arrives at the telescope.
SDP_REQ-642	Transient Buffer Receive Low	The SKA1_LOW SDP shall start recording Transient Buffer data no later than 900 seconds from the time that the highest frequency component of a transient signal arrives at the telescope.
SDP_REQ-643	Transient Buffer Receive	The SDP shall receive Transient Buffer data from the CSP for the purpose of archiving the transient buffer data.
SDP_REQ-644	Pulsar timing compute performance	When performing pulsar timing the SDP shall have at least sufficient performance to execute an algorithm of comparable complexity to using PSRCHIVE (for processing PSRFITS fits files and producing pulsar arrival times) and TEMPO2 (for computing time residuals and updating timing models).
SDP_REQ-645	Pulsar timing quantity	When performing pulsar timing processing the SDP shall be able to process data from 16 pulsars concurrently with SKA1_MID constrained to a net, on sky, bandwidth of 20GHz per polarisation.
SDP_REQ-646	Single Pulse search compute performance	When performing single pulse transient search the SDP shall have at least sufficient performance to execute an algorithm of comparable complexity to using Pulsar Feature Lab (for heuristics), Gaussian Hellinger Very Fast Decision Tree (classification) and Sigproc Gtools (TBC-043) (for coincidence tests).
SDP_REQ-647	Single pulse reception rate	While performing single pulse transient search the SDP shall be able to receive one candidate per beam every 1 second (TBC-044).
SDP_REQ-648	Pulsar search compute performance	When performing pulsar search the SDP shall have at least sufficient performance to execute an algorithm of comparable complexity to using Pulsar Feature Lab (for heuristics), Gaussian Hellinger Very Fast Decision Tree (classification) and Sigproc Gtools (TBC-045) (for coincidence tests).

SDP_REQ-649	Pulsar search performance	While performing pulsar search the SDP shall be able to process a maximum of 1000 candidates per beam.
SDP_REQ-653	Flag invalid data	The SDP shall flag invalid data (NaN or Inf) and data invalid according to metadata.
SDP_REQ-706	Delivery latency	The SDP shall start delivering any science data product, regardless of physical location, within 10 minutes (for a 1TB science product) (TBC-077) of receiving a retrieval request for a science data product.
SDP_REQ-722	TM command acknowledgement latency	The SDP shall acknowledge receipt of commands from TM within 1s.
SDP_REQ-731	Science events	The SDP shall send events to the TM for the following activities: -detection of an imaging transient -detection of a single pulse transient.
SDP_REQ-763	SDP Critical failure identification	The SDP shall identify more than 99% of all critical failures and report them to TM.
SDP_REQ-764	SDP Isolation of critical failures	The SDP, shall isolate 95% of all critical failures and report it to TM.
SDP_REQ-786	Dynamic Spectrum data product	The SDP when commanded shall receive and store a high time resolution dynamic spectrum data product (time-frequency-polarisation).
SDP_REQ-787	Dynamic spectrum sub-array support	The SDP, when configured in dynamic spectrum mode, shall receive and store dynamic spectrum mode data for a total of up to 16 dual polarisation beams (with SKA1_Mid constrained to a net, on sky, bandwidth of 20 GHz per polarisation) from one to sixteen subarrays, independently and concurrently.
SDP_REQ-807	Dynamic Spectrum Mode Data Preparation	SDP shall perform data pre-processing (aggregating sub-integrations from a scan into a single file) for dynamic spectrum mode data for SKA1_Low and SKA1_Mid.