	Standard	Asset Management
---	-----------------	-------------------------

Title: **Management of Plant Software Standard** Unique Identifier: **240-56355910**

Alternative Reference Number: **N/A**

Area of Applicability: **Generation, Engineering**

Documentation Type: **Standard**



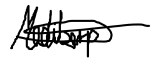
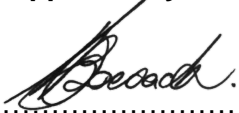
Revision: **2**

Total Pages: **20**

APPROVED FOR AUTHORISATION
☒ GENERATION ENGINEERING
DOCUMENT CENTRE ☎ X4962

Next Review Date: **February 2027**

Disclosure Classification: **CONTROLLED DISCLOSURE**

Compiled by	Approved by	Authorised by
		
Dr. Craig D. Boesack Chief Engineer C&I	K. Sobuwa Chief Engineer C&I	P. Madiba Senior Manager C&I
Date: 17/01/2022	Date: 18-Jan-2022	Date: 2022-01-27
Supported by SCOT/SC/TC		
		
Dr. Craig D. Boesack Power Plant C&I SC Chairperson		
Date: 17/01/2022		

PCM Reference: 240-56355828

SCOT Study Committee Number/Name: Power Plant C&I Study Committee, PP C&I SC08-03

CONTENTS

	Page
1. INTRODUCTION	3
2. SUPPORTING CLAUSES.....	3
2.1 SCOPE	3
2.1.1 Purpose	3
2.1.2 Applicability.....	4
2.2 NORMATIVE/INFORMATIVE REFERENCES	4
2.2.1 Normative	4
2.2.2 Informative.....	4
2.3 DEFINITIONS.....	5
2.3.1 Classification	6
2.4 ABBREVIATIONS.....	6
2.5 ROLES AND RESPONSIBILITIES.....	6
2.6 PROCESS FOR MONITORING	6
2.7 RELATED/SUPPORTING DOCUMENTS	6
3. MANAGEMENT OF PLANT SOFTWARE.....	7
3.1 GENERAL REQUIREMENTS	8
3.1.1 A First Step in meeting Requirements	9
3.1.2 Specific Procedures for the Management of Plant Software	9
3.1.3 Disaster Recovery Plan.....	9
3.1.4 Software Inventory	10
3.1.5 Back-Up or Archive Plan	11
3.1.6 Patch Management Plan	12
3.1.7 Checking / Verifying Updates and Back-ups.....	13
3.1.8 Backed-Up Software Copies	13
3.1.9 Storage of Plant Software	14
3.1.10 Management of Change.....	14
3.1.10.1 Revision register	15
3.1.10.2 DEM Version Updates.....	15
3.1.10.3 Temporary Changes	15
3.1.10.4 Change / Modification Control.....	15
3.1.10.5 Tools for Changes / Modifications.....	15
3.1.11 Communication and Informing users	16
3.1.12 Licensing Issues.....	16
3.1.13 Statutory Requirements.....	16
3.1.14 Impact of other Software on "Controlled Software"	16
3.1.15 Requirements	16
3.1.15.1 Long-term requirements.....	16
3.1.15.2 Medium-term requirements	17
3.1.15.3 Short-term requirements	17
3.2 5 RECORDS.....	17
4. AUTHORISATION.....	18
5. DEVELOPMENT TEAM	18
6. ACKNOWLEDGEMENTS	18

FIGURES

Figure 1 – Software Management Procedures and Integration to Plant Hardware.....	7
Figure 2 – Software Backup Strategy	12

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

1. INTRODUCTION

The Management of Plant Software Standard sets forth minimum requirements and guidelines necessary for the administration and management of Power Plant Control and Instrumentation Software. The term Software delineates and characterises all Software forming part of Control System technologies, essential for the functioning and operation of hardware systems according to its specific control objective.

This includes Software for Engineering (Engineering and Programming Tools), Control System Software for Logics (Control Logics for Analogue and Digital Control Systems), Software for Hardware Programming and Embedded Software for Real-Time Control Systems (such as Firmware), Specific Software (for Field Devices, its management and control) and Software for the Management of Networked Components.

It is clearly seen that Software covers a wide range of technologies and applications, ranging from Software for the management of Field Devices, through Control Systems (PLCs's, DCS's and Standalone Controllers) to the Software required for the Visualisation and Control of Control System Technologies (such as SCADA, HMI, and Operator Panel software). Although it is impossible to describe all Software and its applications to Control Systems, these mentioned above form the basis of most automation Control Systems.

Since modern Power Plants are complex systems composed of highly integrated Control Systems, varied in technology and application software, the effective Management of Plant Software is required. Therefore, this Standard is developed in response to the need to provide minimum requirements for the Operation and Maintenance practice of Control System Software for Power Plants.

Strong focus is given to Control & Instrumentation Systems, its infrastructure, and the mechanisms by which these systems are managed and administered. In line with Eskom's business objectives for efficient equipment life cycle management and improving control system reliability and availability, it is beneficial to guard against performance deterioration of C&I Systems and to minimise risk through the application of best practices. This is particularly true for disaster recovery and Control System Restoration instances after failure.

Therefore, the Management of Plant Software Standard is aimed at providing minimum compliance criteria for Power Plant Owners for the Management of Plant Software.

2. SUPPORTING CLAUSES

2.1 SCOPE

The scope of this Standard is to provide best practices for the Management of Plant Software at Eskom's power plants. Due to the extensive range of technologies utilised at various sites, this Standard defines the process and methodologies that should be considered when managing plant software and suggest methods for improvement and best practice guidelines for the management of Software.

In addition, although this standard contains information of relevance to Cyber Security, a specific document addressing Cyber Security in its entirety shall be developed and followed.

2.1.1 Purpose

It is the purpose of this Standard,

1. To facilitate the recovery of Software in the event of the loss or degradation of the Software due to adverse site conditions, e.g., unsuccessful modification, disk damage, fire, misplacement, etc.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

2. To provide a viable method for Engineering and Maintenance Staff to maintain and modify Software if necessary.
3. To provide a method for recording software changes and providing an efficient software version tracking system.
4. To maintain the quality and integrity of Software used on the Plant and complement the long-term health of the Plant by facilitating the speedy recovery of Control Systems after failure.
5. To ensure that Eskom can process any dispute during the guarantee period following the take-over of the new Plant with its Software.
6. To form a guideline for the management of Software for New and Refurbished C&I projects to ensure the continuity of Software Management.

2.1.2 Applicability

This Standard applies to:

1. All Power Plants forming part of the Generation Fleet, all Units, Common Plant and Water Treatment Plants.
2. All Software based systems in the Control and Instrumentation environment including Process Control, Monitoring, HMI Systems, Software forming part of Networked Control Systems and Engineering Tools.

2.2 NORMATIVE/INFORMATIVE REFERENCES

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.2.1 Normative

- [1] ISO 9001 Quality Management Systems.
- [2] Eskom Cyber Security Standard for Operational Technology, 240-55410927.
- [3] The Management of Plant Simulations Standard, 240-56355904.

2.2.2 Informative

- [4] 32-385 (IT Continuity / DR Standard).
- [5] Eskom IT Disaster Recovery Strategy, 240-47615255.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

2.3 DEFINITIONS

Administrator	An appointed person who will administer the Application software.
Application Software	Applications Software (also called end-user programs) includes database programs, word processors, and spreadsheets. Figuratively speaking, applications software sits on top of systems Software because it is unable to run without the operating system and system utilities.
Archive copy	The archive copy is stored at long intervals, typically a year or two. The archive copy is updated only from the controlled copy. The software integrity must be verified before the controlled copy is used to overwrite the archive copy.
As Commissioned	The term as commissioned" refers to the condition of the Software on the day that the Plant was finally commissioned. No modifications have been done on this Software.
Controlled copy	The controlled copy is stored at shorter intervals typically around four to six months.
Controlled Software	The Software applicable to this Manual. This specifically includes Software used on the Plant that is necessary for the normal operation of the control systems.
Hand-over copy	Software handed over to ESKOM after commissioning. This Software is as commissioned and will be used as a master reference during the life of the Power Station.
Maintenance copy	The maintenance copy is the copy of Software that is identical to the Software currently used on the Plant. It is stored regularly or only on modifications. The system engineer decides upon an applicable update interval.
Plant Software	Plant software refers to all control system software, it includes application software and automation software, used for the control, operation and monitoring of power plant systems.
Set	A set will comprise of relevant Software stored on it for system with comments (if applicable) and the relevant documentation, marked with uniquely identifying descriptions of the control system. (KKS numbers if used).
Software Criticality	Software used on the Plant that is critical to the operation of the Plant. The system engineer is responsible for classifying Software of a specific plant as critical.
Software	Computer instructions or data Anything that can be stored electronically is Software. The storage devices and display devices are Hardware. Software can be divided into two general classes: Systems Software and Applications Software.
Storage device	The device used to store Software on a storage medium.
Storage media	The actual media used to store the Software on. These could be hard drives, magnetic tapes, CD/Rs or DVD/Rs. The technology is dependent on the systems installed. The technology selected should offer the best long-term Storage possible.
System engineer	An appointed person (in writing) from the Engineering Department who will implement the control of Software. This responsibility can be delegated to someone specifically if needed. But it is recommended that a single person be accountable for the integrity of Software.
System Software	Systems Software consists of low-level programs that interact with the computer at a very basic level. This includes operating systems, compilers, and utilities for managing computer resources.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

2.3.1 Classification

- a. Controlled Disclosure: Controlled Disclosure to External Parties (either enforced by law, or discretionary).

2.4 ABBREVIATIONS

Abbreviation	Description
C&I	Control and Instrumentation
CPU	Central Processing Unit
DCS	Distributed Control System
GBE	Generation Business Engineering
HMI	Human Machine Interface
LAR	Limited Access Register
OEM	Original Equipment Manufacturer
PLC	Programmable Logic Controller
PSM	Power Station Manager

2.5 ROLES AND RESPONSIBILITIES

The responsibility to implement this document will lie with Generating Units responsible for the Engineering and Maintenance of Control and Instrumentation Infrastructure at Power Plants.

In addition, there are relevant stakeholders of Project Engineering where C&I Projects are implemented as part of C&I Refurbishment, C&I Modification and any other C&I Projects. Plant Engineering and various Centre of Excellence (CoE's) departments also form part of the stakeholders responsible for the management of Software.

2.6 PROCESS FOR MONITORING

The implementation of this document will be monitored by the Control Systems Care Group and the C&I Study Committee under SCOT and will monitor the implementation of the Standard across the Generating Fleet.

2.7 RELATED/SUPPORTING DOCUMENTS

None.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

3. MANAGEMENT OF PLANT SOFTWARE

The Management of Plant Software Standard provides minimum requirements for the administration, management, Backup and restoration of Power Plant Software for Control and Instrumentation Systems. All Plant Software necessary for the functioning and operation of Control System technologies are to be managed effectively to enable the successful recovery or restoration of Control Systems, such as DCS's, PLC's, HMI's and networked components forming part of the Control System solution, in the event of equipment failure.

The need for highly available and reliable power plant control systems amidst various operational risks continue to increase. Control System performances for continued production and effectively managing these systems well in the presence of technical risks introduce performance requirements for Power Plant Management, Operations and Maintenance.

The following factors greatly impact the performance, availability and reliability of Power Plant Control Systems.

- Failure of Control System Hardware and Components.
- Equipment failure due to Human Error.
- Malware, Viruses and Cyber related attacks on Control System technologies.
- Control System design errors, modification leading to failure and errors introduced by malpractice.
- Network Failures.

Figure 1 gives an overview of software management and the systems necessary for effective management of plant software.

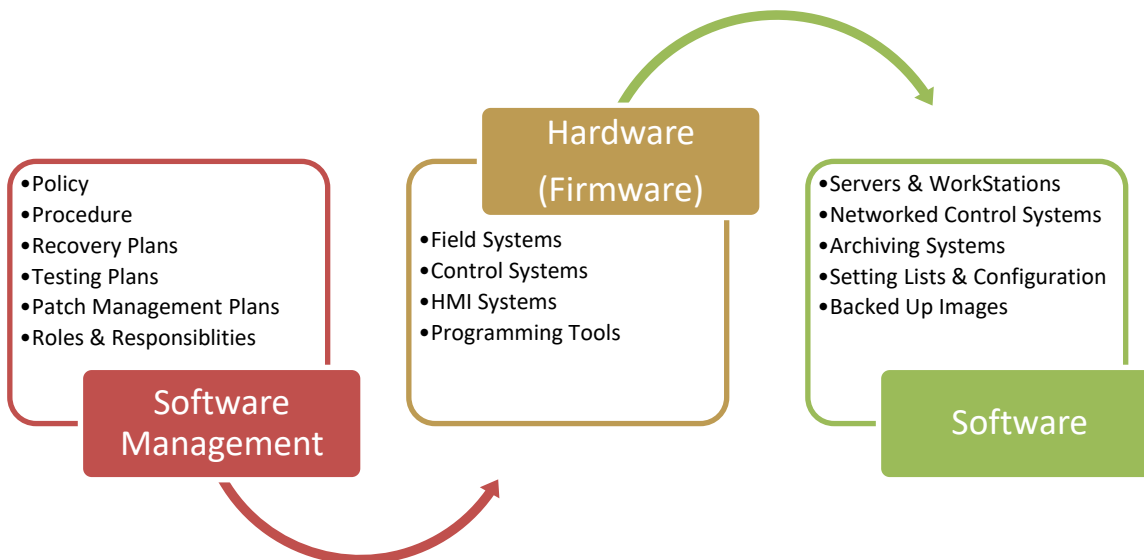


Figure 1 – Software Management Procedures and Integration to Plant Hardware

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

Each of the items above directly or indirectly results in a deterioration of Power Plant Control System performance, impacting Plant availability and downtime. This essentially motivates the Management of Plant Software Standard to mitigate against the abovementioned risks, events and threats mentioned with the express intent for rapid recovery and restoration of Plant Control Systems.

Effective management of plant software consists of a holistic approach to the maintenance management of control system software, tools, and systems. These aspects work together to ensure a speedy recovery of control systems after system hardware or software failure. Critical criteria for successful implementation of the management of Software consist of:

1. Maintaining a high level of compliance to established policy, standards and procedures relating to the management of control system software.
2. Regularly confirm plant software integrity and have validated recovery strategies of systems in place.
3. Employing effective system administrative training and maintenance programs to ensure skilled plant personnel manage plant software.

3.1 GENERAL REQUIREMENTS

The Management of Plant Software is essential for safe and reliable Power Plant Operation and Control. Still, more importantly, it provides a framework for managing, controlling, and performing recovery operations of Control Systems when the need arises. In numerous cases, Plant Software is not managed well, which presents a risk to Operations and the availability of Generating Units. However, by effectively managing Software, high integrity and confidence in recovery efforts can be obtained, and the Plant can be returned to normal production within minimised time frames.

Power Plant Software and its application cover various technologies, systems, and solutions specific to each Power Plant. It is impossible to fully describe all Control System technologies and their respective nuances within this document, but the management principles of how the Software should be managed, administered and how policy, processes, and procedures with roles and responsibilities are comprehensively described within this Standard.

The Management of Plant Software Standard focuses on the following key areas, with the express intent to plan for disaster and have a recovery strategy for Control Systems. Therefore, effective planning and preparation are necessary to mitigate the failure effects of Control System technologies.

Under the auspices of C&I Maintenance and C&I Engineering, the Power Station is accountable for the Management of Plant Software. Their respective scope of responsibility shall include all Control System Software for the Power Islands, Units and Common Plant, including the WTP. The Management of Plant Software Standard aims to present minimum requirements practical throughout the Life Cycle of Plant Software.

In addition to the General Requirements, there are Specific Requirements for managing Plant Software; these are described hereafter. The requirements intend to ensure that in the case of Control System Plant Software problems, the recovery of the Control Systems can be achieved within the shortest durations, ensuring that system reliability, availability and the Control System integrity is maintained.

The following sections capture the minimum requirements necessary to be addressed, fulfilling the General Requirements of the Standard.

CONTROLLED DISCLOSURE

3.1.1 A First Step in meeting Requirements

The first step in meeting the Management of Plant Software Standard is to assess the status of Plant Software. This involves gathering knowledge of the relevant control system, its Software and applicable recovery procedures. This also includes assessing the administration tools required for recovery and processes and validating them to ensure proper functioning.

The assessment shall consist of the following:

1. The software system assessment shall be recorded in a register and documented.
2. Identifying the critical importance of control systems and assessing how long the Plant can operate without the control system running. There are many control systems within power plants, some controlling highly sensitive processes, such as boilers and turbines critical to power plant operations. Similarly, there are fewer essential processes that can afford lower recovery importance. Therefore, a detailed assessment of control system criticality shall be performed to define the need for software management and how it shall be managed.
3. A comprehensive list of all control system software shall be compiled and documented.
4. A comprehensive list of all control system recovery procedures shall be documented.

3.1.2 Specific Procedures for the Management of Plant Software

The Management of Plant Software Standard calls for the effective administration of all types of Control Systems Software, of Hardware (in the form of Firmware, where applicable), and of Software for Managing Control Systems Hardware, its operations, and its control. This can be very broad in its application, but the methodology for managing Plant Software at the Power Station must be compiled and effectively performed. This responsibility resides with the Power Station, responsible for developing Site Specific Procedures for the management and administration of Control System Plant Software. These procedures shall be developed in accordance with best practices, with allotted Roles and Responsibilities documented and known.

1. An inventory of Plant Specific Procedures shall be kept (as specified within this Standard).
2. Procedures shall be written in accordance with OEM specific guidelines where procedures apply to specific technologies.
3. A Roles and Responsibility Matrix of site personnel who administers Plant Software shall be kept and effectively communicated.
4. Specific System-Back-Up and Restoration Procedures shall be kept controlling the process of Back-Up and Restoration of Control Systems in accordance with this Standard, OEM specific procedures and best practice.
5. Procedures shall be authorised and registered according to formal documentation procedures at the Power Station.

3.1.3 Disaster Recovery Plan

The Station shall maintain a Disaster Recovery Plan (DRP) for all the Control Systems and their respective components and devices. The Disaster Recovery Plan typically captures all the information necessary, as well as the processes for performing a disaster recovery and the roles and responsibilities involved in the processes; the DRPs shall be contained within a single repository and duplicated in another controlled location only accessible by the responsible persons involved in the backup and disaster recovery procedures and related processes. The Power Station shall DRPs for each of the Control Systems applicable to the functional areas.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

For the Disaster Recovery Plan to be effective, it shall be based upon a team concept, with specified Roles and Responsibilities, with knowledgeable and experienced personnel capable of performing the recovery task.

The Disaster Recovery Plan shall consider the following areas as a minimum.

1. Control System Software (PLC's, DCS's & Standalone Controllers).
2. Control System Network Infrastructure.
3. Control System Server Infrastructure.
4. HMI and SCADA Systems,
5. Data Storage and detailed Backup Systems.
6. Field Installation Infrastructure, including field-related engineering tools and Software.
7. Role and Responsibilities, clarified and known by the responsible persons.
8. Detailed Recovery Procedures.
9. Detailed Validation Testing Procedures.
10. Equipment and System Requirements lists of Hardware, Firmware, Software, settings, and configurations (Hardware and Software) and other resources necessary to support system recovery operations.
11. Testing Procedures and Maintenance Procedures.

The Disaster Recovery Plan of a Control System will guide the restoration of the control system functionality and ensure that operations are normalised within a minimum time frame.

Therefore, the plan shall identify vulnerabilities and recommend necessary control measures in the DRPs to facilitate system recovery.

3.1.4 Software Inventory

A comprehensive inventory list of all Control Systems Plant Software shall be kept, managed, and updated. When Software is modified, new Control Systems are added and keep track of Software Versions. Although not limited to the following, an accurate assessment of Control System Plant Software needs to be made, considering its importance and criticality to Process Control, influence on production and availability of Control Systems.

1. Software for Field Devices – Software for Field Devices shall be effectively managed; such systems include Pressure Transmitters, Actuators and Programmable Field Devices.
2. Examples of Software for Field Devices include:
 - a. Instrument Calibration Software Tools (such as HART).
 - b. Instrument Setting Lists.
 - c. Instrument programming tool software, programming units (PGs), and laptops are used for instrument maintenance.
3. Plant Software for Control Systems – Plant Software for the Control Systems shall be effectively managed; such systems include PLC's, DCS's (and associated infrastructure) and Standalone Control Devices.
4. Plant Software for Networked Control System Components – Plant Software for Networked Control Systems shall be effectively managed; such systems include Network Switches, Routers and Gateways, Networked Servers and Workstations, and Software for Plant Archiving Systems.
5. Plant Software for Control System HMI and SCADA Systems – Plant Software for Control Systems HMI and SCADA shall be effectively managed; such systems include HMI Thin Clients, SCADA Control System Hardware and Software, and Local HMI Panel Software

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

6. Based upon the Control System topology, its function and design, all elements of the design fundamental to control functioning shall be evaluated and assessed, with comments on relevance to Hardware Firmware and Software criticality. A document highlighting this process shall be kept for record purposes.
7. Critical Software includes, but is not only limited to these are:
 - a. Unitized PLC/DCS and SCADA Software.
 - b. Standard Plant Systems Software.
 - c. Automation and Application Server Software.
 - d. Software used to perform Maintenance/Engineering functions.
 - e. System databases and system restoration files.
8. Accompanied with this, a detailed Risk Assessment of Plant Software should be kept, highlighting the risk this Plant Software poses to the Availability, Reliability and Safety of Plant Operations (in the event of software failure, and importance to recovery operations).

3.1.5 Back-Up or Archive Plan

The Station shall regularly maintain a current and functional Backup or Archive of Plant Software. It is recommended that incremental back-ups be kept and are weekly performed. Automated back systems may have a daily update frequency. Depending upon the nature of the control system, PLC's, standalone controllers, SCADA systems, or DCS's a regular and current Backup shall be kept.

The Software Back-Up shall be a "good" snapshot of the functional elements of the Control System and shall, upon Restoration, lead to a fully operational Control System and production system. This inevitably requires that there be a Backup or Archive Plan. The Back-Up or Archive Plan shall, as a minimum, describe.

1. The frequency of the Backup. Ensure that all files, Software, including system files, images are backed up regularly, on a systematic basis (including full and incremental back-ups).
 - a. Full Back-ups – Full Backup refers to the Backup of the entire system, such as all volumes of a server or control system). One of the limitations of the full Backup is that disk space required for Backup is large and it can be a time-consuming exercise. However, there can be a certain amount of compression to optimise backup Storage.
 - b. Incremental Back-ups – Incremental back-ups store only newly created or updated data since the last backup operation. This saves storage media space in contrast to full back-ups.
 - c. The methodology for system backup is to follow a Full Backup + Incremental Backup approach to systems (Figure 2).

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

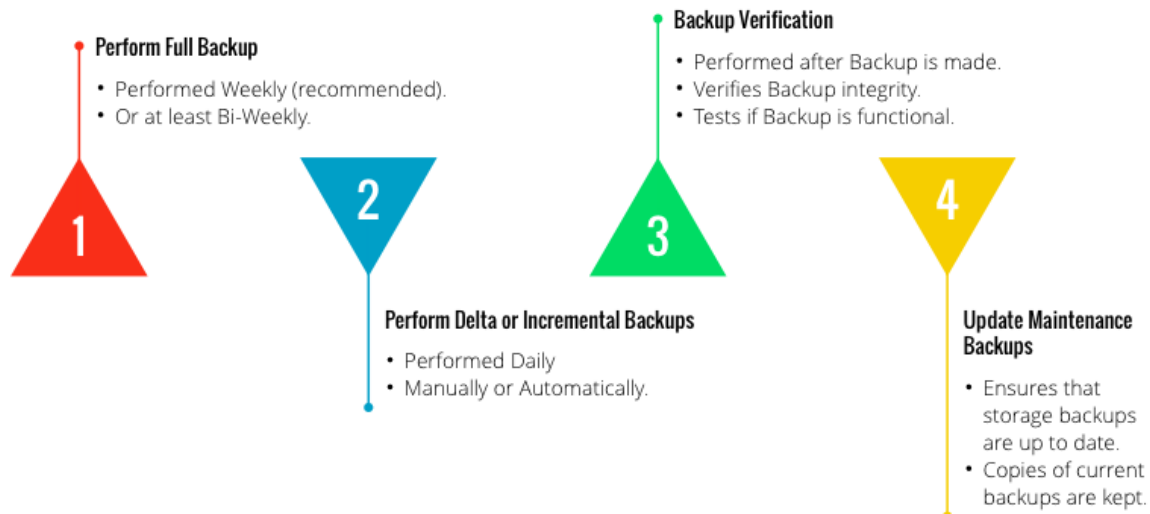


Figure 2 – Software Backup Strategy

2. Back up the entire system when making software changes, such as upgrades, modifications, or major modifications.
3. The process and functional requirements necessary for the creation of the Backup.
4. The process and procedures are necessary for verifying the Backup.
5. The validity period of the Backup, from the time of Backup creation, a new Backup of the Control System needs to be made.
6. The method of physical Storage of the Backup. This shall include Back-Up Storage Locations, Number of Backup Copies and Backup environmental requirements.
7. Testing of Back-Up shall also be performed, and this is to be documented within the Backup Plan. (See Recovery Plans for Additional Requirements).
8. Software back-ups must support the OEM recovery strategy for the relevant system.

3.1.6 Patch Management Plan

The Power Station shall maintain a Patch Management Plan. The Control System Software Patches aim to improve the functionality and stability of the Control Systems and, more recently, have been focused on enhancing the security of the Control Systems technology. However, since patches can impact the availability of the Control Systems, it is necessary to have a comprehensive Patch Management Plan and process per Control System as supported by the OEM; elements of the plan shall consist of the following.

1. Regular Vulnerability Assessments shall be performed following the CSSO by knowledgeable personnel authorised to perform this function.
2. An inventory of Hardware of all the control systems equipment, with a cross referenced list of current and up-to-date software versions.
3. An archive of the Plant Software prior to the implementation of the Patch shall be maintained, a Hardware Inventory, current configuration and schematics of the Control System shall be retained as well.
4. Documentation detailing the system design and documenting the configuration baseline.
5. The patch applicability reporting, showing the impact and vulnerability procedures, are clearly documented.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

3.1.7 Checking / Verifying Updates and Back-ups

The Backup and Recovery Plans refer to the various strategies and procedures required to protect and recover from Control System failures. The Backup shall be fully functional and current for the operational application when needed.

Therefore, to ensure that the recovery process is successful, it is necessary for the Procedures and Backup's to be checked and verified routinely and after the modification of the Plant Software.

Thus, the Control System Administrator Shall Test, Document, and Verify all Plant Software and periodically review the Backup and Restoration processes and procedures to ensure that Backup integrity is maintained. The following shall be carefully considered during Checking and Verification.

1. A Checking / Verification Plan shall be maintained and ensure fast recovery of failed Control Systems and thoroughly tested.
2. The integrity of the Plant Software on Back-Up shall be routinely tested by applying the Restoration procedures and documented within the Checking / Verification Plan.
3. It is required that the Plant Software (of System and Application) integrity be verified. This task is only to be performed if a low-risk test can be performed and does not pose a risk to production operation (e.g., do not test Software on a live plant, utilise outages of sufficient duration such as to not delay the coming back of the Plant and or unit).
4. If software back-ups differ from the Plant Software used on the Plant to such an extent that it cannot be easily modified to work on the Plant anymore, an update should be done to have at least three usable copies of the current Software.
5. When updating Plant software systems and Operating Systems software, verify that all necessary files are backed up, including hidden and system files in other directories that might be important to the functioning of the Software.
6. Attention should also be given to the specific technology used for the storage media and the particular manufacturer's recommendations regarding data verification and expected life.

3.1.8 Backed-Up Software Copies

Plant Software shall be backed-up, and at least two backup copies shall be made. These shall follow the requirements described below.

1. Hand-over copies are the set of Plant Software delivered to ESKOM after the Process Control System has been commissioned. This set is kept as a reference and will never be changed.
2. Three operational sets of Plant Software shall be kept for each control system. These sets (or copies) are updated at certain intervals. Backed-Up copies are updated regularly after full back-ups are made.
3. The maintenance copy is the most recently updated copy and should be kept identical to the Software used on the control system. Every four to six months, the maintenance copy should be verified and copied to a set of plant Software called the controlled copy.
 - a. The backup verification process confirms that the backup procedures are current and functional.
 - b. Secondly, backup verification ensures that the Backup is functional and that problems in the backup procedure can be identified, understood and any "bugs" identified and corrected.
 - c. The backup verification process facilitates recovery and may take just as long as the making of the Backup. The verification process reads and confirms all the Checksums on the media to verify that data has been correctly written to the storage media (typically, this process is performed immediately after the Backup is performed). The Checksums also validates that the Backup on the media is intact.

CONTROLLED DISCLOSURE

- d. The backup verification process also confirms the actual storage media and whether the backup files are either incomplete, inaccessible, or unreadable.
4. The controlled copy is the second level of Software. It is not necessarily identical to the Software on the plant Control System. The controlled copy is only updated from the maintenance copy at the specified intervals the system engineer decides.
5. Every year to two years, the controlled copy is verified and copied to the archive copy (depending on the storage medium). This Plant software will only be used when the maintenance copy and controlled copies are destroyed or unavailable.
6. It is good practice to keep the different copies of Software in different locations and store them in appropriate environmental conditions as recommended by the manufacturer of the storage medium. This minimises the risk of destruction by fire and other localised threats such as dust and magnetism. It is also recommended that different levels of access control be exercised with the three sets of Software to minimise tampering.

3.1.9 Storage of Plant Software

Plant software's Storage and its methods should be following OEM recommendations and best practices. They should be kept in a location that will not be affected by disasters. Particular attention should be given to the Storage Location, Fireproofing, Environmental Storage Conditions (such as temperature and humidity), and the storage medium's data life.

The Storage of Plant Software Copies should be separate from the Control System locations and housed at a different location.

The following form recommended storage practice.

1. Software shall be stored On-Site and Off-Site; the redundancy of storage locations minimises common disasters from affecting copies of backed up Plant Software.
 - a. One of the guiding principles between On-Site and Off-Site is that backups should be stored in different locations. In some cases, control system Plant Software, back-ups and recovery are managed as part of OEM Service Level Agreements (SLA's), in which case Plant Software is stored Off-Site forming part of the OEM facilities.
 - b. Off-site also means that backup Plant Software is not stored in the same area of the technology or where Software is kept; it can be at different rooms at the Station (it offers redundancy of Storage). The storage locations of the backup Plant Software shall be effectively managed.
2. One full set of Plant Software Copies is to be stored On-Site for immediate recovery of Control Systems.
3. While, another copy of Plant Software is to be stored Off-Site in the case of fire, theft and any other disaster.
4. Plant Software should be retained until a system is decommissioned fully and no possibility exists that the control system will be used again.

3.1.10 Management of Change

A comprehensive change management process shall be followed for the Plant Software. This aims to prevent and detect unauthorised changes or modifications to Plant Software and align with the Engineering Change Management Processes.

In addition to this, requirements are stipulated for protecting Plant Software from being compromised that could lead to malfunction or incorrect operation of Plants due to incorrect Software being loaded during the disaster recovery.

The roles and responsibilities of the control system administrator (or all personnel) who manage plant software shall be regularly reviewed and confirmed. In cases where the person who works with plant software is no longer an employee or a responsible person for Plant Software, their

CONTROLLED DISCLOSURE

roles relating to software management shall be removed. This includes the management of Plant Software during the construction projects also.

Therefore, as a minimum, the following form's part (but not limited to):

3.1.10.1 Revision register

The revision register is a document that keeps track of all the different revisions of Software. The revision register is updated every time software is changed permanently (not for simulations or I). This document should also be linked to the local power station modification configuration system.

The revision register should, as a minimum, contain the following information:

- Name of the system which Software changed,
- Date of change,
- Reason for change,
- Name of the person implementing the change
- A detailed description of the change.

3.1.10.2 DEM Version Updates

A record should be kept of versions of OEM system software used on the Plant. This will help recover the correct version from the OEM in a critical event. Regularly confirm that the versions of Plant Software used on the Plant are available from the OEM. Information to be recorded are the date of the last update, serial numbers, licensing and OEM contact information, and the person involved in the update/upgrade of the Plant Software.

3.1.10.3 Temporary Changes

If any temporary changes are done to software (e.g., tests) a separate maintenance copy should be kept having an "up to date copy" available for disaster recovery. The temporary software change should not interfere with the normal backup system and should not propagate into the controlled copies and archived copies.

In cases of simulation, all plant software simulations shall be managed in accordance with the official simulation standard and station simulation procedure.

3.1.10.4 Change / Modification Control

This Standard accepts that the modification process drives software changes. Authorisation of modification falls out of the scope of this Standard. Changes not forming part of the modification process like "tuning" should not propagate into the normal maintenance copies, controlled copies and archive copies.

Software changes shall follow the ECM process. Optimisation settings must be backed up as part of the maintenance copies after proven plant performance.

3.1.10.5 Tools for Changes / Modifications

Software used on site-specific engineering tools like engineering stations, handheld programmers, and programming units, should be backed up separately to ensure the long-term usability of the tools. The backing up of this Software is the responsibility of each site and must

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

follow the guidelines presented in this Standard, although the procedures are system and site-specific.

3.1.11 Communication and Informing users

All software users should be informed of the changes on the documentation and should also be made aware of the current maintenance copy. If any other documentation is updated, the documentation should be forwarded to all relevant parties. Specific regard should be given to where there are differences between multiple applications of similar Software such as on the six or more power station units.

3.1.12 Licensing Issues

Licensing of Software should be maintained especially if it changes during a modification. Licence numbers and serial numbers should be kept assisting in recovering a licence. A process should also be set up to cater for the event of a licence loss specifically. Hardware copies of licences (if it exists) should be kept proving ownership of a specific software licence.

3.1.13 Statutory Requirements

These guidelines may not be applied in such a manner as to contravene the requirements of any other statutory regulations, with specific reference to the Copyright act and Software licensing and piracy aspects.

3.1.14 Impact of other Software on "Controlled Software"

Attention should be given to loading un-controlled Software onto the same computer system as controlled Software (e.g., file utilities, games, personal programs, etc.). The installation and uninstallation of this uncontrolled Software could degrade the controlled Software, especially system software. It is not good practice to load uncontrolled Software on Plant Control Systems, and it should be avoided.

3.1.15 Requirements

Various requirements exist in establishing an effective software control system, which is significantly enhanced by experienced System Administration and by fulfilling the functions specified within this Standard. The approach to successfully applying the Management of Plant Software Standard is to be driven through effective Maintenance and Engineering processes, following good practices. These requirements are grouped as follows:

3.1.15.1 Long-term requirements

- a. Ensure that this software control standard is implemented and controlled by the Responsible Person.
- b. Keep the Hand-over and Archive sets in a safe fireproof environment.
- c. Ensure the continuity of this Standard when a new Responsible Person is appointed.
- d. Auditing of this software control standard as applied at the power station to ensure its effectiveness and identify possible shortcomings.

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

3.1.15.2 Medium-term requirements

- a. Implement this Standard and associated site-specific procedures and control software changes so that the integrity of the Software be maintained.
- b. Verify the maintenance copies of the Software every four to six months or deemed necessary by the responsible person.
- c. Keep a record of all the software changes on the Plant in a file dedicated for that. It is recommended to keep electronic copies of records on file.
- d. Update any hard copies of documentation regularly, six-monthly.
- e. Dedicated plant maintenance procedures regarding Plant Control System Software Management based on the requirements of this Standard shall be compiled and registered for the necessary work.

3.1.15.3 Short-term requirements

- a. Ensure proper awareness and training of this Standard.
- b. Ensure that personnel synchronise changed Software on all the relevant programming units or other engineering tools.
- c. Log all changes to Software so that the differences will be apparent to everyone.
- d. Update the maintenance copies regularly and after any changes.
- e. Always ensure compliance with this Standard.

3.2 5 RECORDS

The records to be kept are listed as follows.

- a. Revision register.
- b. Procedure records (for the management of this Standard and related procedures).
- c. Licence records (licences, hardcopy proof, and serial numbers).
- d. A detailed asset register shall be provided. The register shall include a description of the equipment, tag reference, classification of risk associated with the system's failure. Records and registers shall be kept on an archived Server.

Records must be kept until the Plant is decommissioned or until the currently installed application has been entirely replaced with a new system with its Software.

CONTROLLED DISCLOSURE

4. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
Andrew Botshe	Manager: C&I (Generation)
Christoph Kohlmeyer	Chief Engineer: C&I
Cornelius Visagie	Chief Technologist: C&I
Jorge Nunes	Chief Engineer: C&I
Khaya Sobuwa	Chief Engineer: C&I
Paul Du Plessis	Chief Technologist: C&I
Prudence Madiba	Senior Manager: C&I
Zubair Moola	Chief Engineer: C&I

Revisions

Date	Rev.	Compiler	Remarks
November 2012	A	J Viljoen	Draft Document for review created from 36-194 for TDAC
September 2016	0	CD Boesack	Added additional paragraphs and content final Draft
January 2017	0.1	CD Boesack	Final Draft for Comments Review Process
February 2017	0.2	CD Boesack	Final Updated Draft after Comments Review Process
February 2017	1	CD Boesack	Final Document for Authorisation and Publication
January 2022	1.1	CD Boesack	Minor updates for renewal.
January 2022	1.2	CD Boesack	Final Draft after Review Process
January 2022	2	CD Boesack	Final Rev 2 Document for Authorisation and Publication

5. DEVELOPMENT TEAM

The following people were involved in the development of this document:

- Dr Craig D. Boesack
- Control Systems Care Group

6. ACKNOWLEDGEMENTS

- Jorge Nunes
- Corneluis Visagie

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

Appendix 1 – Minimum Documentation Requirements

#	Required Documents	Standard Clause/Page	Check
1.	Plant Software Assessment	3.1.1/8	<input type="checkbox"/>
2.	Specific Procedures	3.1.2/9	<input type="checkbox"/>
3.	Disaster Recovery Plan	3.1.3/9	<input type="checkbox"/>
4.	Comprehensive Software List	3.1.4/10	<input type="checkbox"/>
5.	Backup Strategy or Plan	3.1.5/10	<input type="checkbox"/>
6.	Patch Management Plan	3.1.6/12	<input type="checkbox"/>
7.	Software Revision Register	3.1.10.1/14	<input type="checkbox"/>
8.	OEM System Software	3.1.10.2/14	<input type="checkbox"/>
9.	Records of Software Licenses	3.1.12/15	<input type="checkbox"/>

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

Appendix 2 – Maintenance Software Management Overview

Activates	DCS	PLC	Networks	HMI	SCADA	Standalone systems	Field devices	PIS	Station PM reference
Back ups									
Working copy	*	2	*	*	*	2	2	2	
Maintenance copy	2	2	2	2	2	2	2	2	
Archive copy	3	3	3	3	3	3	3	3	
Verifying back up									
Working copy	*	2	*	*	2	2	2	*	
Maintenance copy	2	2	2	2	2	2	2	2	
Archive copy	3	3	3	3	3	3	3	3	
Recovery verification	3	3	3	3	3	3	3	3	
Change management									
Revision control	2	2	2	2	2	2	2	2	
Patch updates	1	2	1	1	1	2	2	1	
Virus protection	1	2	1	1	1	2	2	1	
OEM revision control	2	2	2	2	2	2	2	2	
Review simulation	1	1	3	3	2	2	2	3	
Review OT asset register	2	2	2	2	2	2	2	2	
Period reference									
six months	1								
Yearly	2								
2 Yearly	3								
During GO	4								
*	Not required								

CONTROLLED DISCLOSURE

When downloaded from the EDMS, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.