Eskom	Standard	Technology

Title: **Management of Plant Software Standard**

Unique Identifier:	**240-56355910**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Engineering**
Documentation Type:	**Standard**
Revision:	**1**
Total Pages:	**20**
Next Review Date:	**February 2022**
Disclosure Classification:	**CONTROLLED DISCLOSURE**

APPROVED FOR AUTHORISATION
☑ TECHNOLOGY ENGINEERING
DOCUMENT CENTRE ☎ X4962

Compiled by

.....

Dr. Craig D. Boesack
Chief Engineer C&I Governance
Date: 16/02/2017

Approved by

.....

K. Sobuwa
Middle Manager C&I Governance
Date: 16/02/2017

Authorised by

.....

P. Madiba
Senior Manager EC&I
Date: 16/02/2017

Supported by SCOT/SC/TC

.....

K. Sobuwa
Power Plant C&I SC Chairperson
Date: 16/02/2017

PCM Reference: 240-56355828
SCOT Study Committee Number/Name: Power Plant C&I Study Committee, PP C&I SC08-03

CONTENTS

FIGURES

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 (PLC'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 not possible to describe all Software and its applications to Control Systems, these mentioned above forms 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.

In particular, strong focus is given to Control & Instrumentation Systems, its infrastructure and the mechanisms by which these systems are to be managed and administered. In line with Eskom's business objectives for efficient equipment life cycle management and on 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 practice. This is particularly true for instances of disaster recovery and of Control System Restoration 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 practice for the Management of Plant Software at Eskom's power plants. Due to the extremely wide range of technologies utilised at various sites, this standard defines the process and methodologies that should be considered when managing plant software, and suggests methods for improvement and best practice guidelines for the management of software.

This standard does not specifically apply to the storage and archiving of historical plant data information (e.g. actual measurements and other such data captured from the plant). In addition, although this standard contains information of relevance to Cyber Security, and 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.
2. To provide a viable method for Engineering and/or Maintenance Staff to maintain and if necessary modify Software.
3. To provide a method for recording changes to Software and to provide an efficient software version tracking system.
4. To maintain the quality and integrity of Software used on the Plant, and to complement the long term health of the plant by facilitating the speedy recovery of Control Systems after failure.
5. To ensure that Eskom is in the position to process any dispute during the guarantee period following take-over of new plant with its software.
6. To form a guideline for the management of software for New and Refurbished C&I projects in order to ensure the continuity of Software Management.

2.1.2 Applicability

This standard is applicable 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.

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 particular 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.

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 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.

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 in order 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 performance, availability and reliability of Power Plant Control Systems are greatly impacted by the following factors;

- 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.

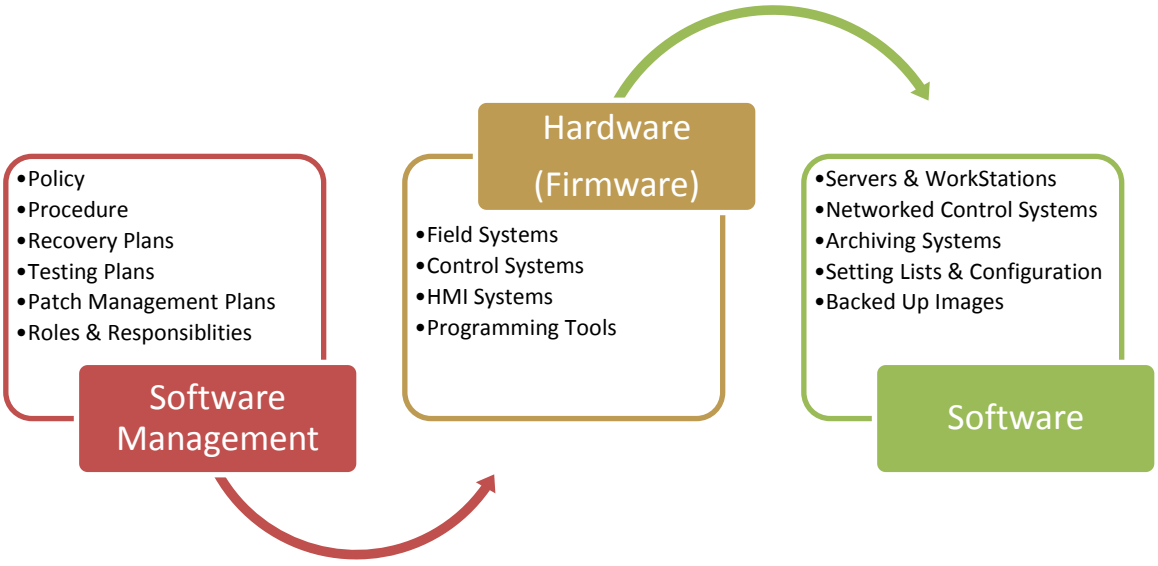

Figure 1 Software Management Procedures and Integration to Plant Hardware

Each of the aforementioned items directly or indirectly results in a deterioration of Power Plant Control System performance, which could impact on Plant availability and downtime. This to a large extent 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. Each of these aspects work together to ensure a speedy recovery of control systems after system hardware or software failure. Key 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 confirming the integrity of plant software, and having 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, but more importantly, it provides a framework for managing, controlling and of performing recovery operations of Control Systems when the need arises. In numerous cases, Plant Software is not managed well, and this presents a risk to Operations and to 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 return to normal Production within minimised time frames.

Power Plant Software and its application cover a very broad spectrum of technologies, systems and solutions, and this is specific to each Power Plant. It is not possible to fully described all Control System technologies and their respective nuances within this document, but the management principles of how the software should be managed, administered, and of 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 for planning for disaster and having a recovery strategy in place for Control Systems. Therefore, effective planning and preparation is necessary to mitigate on the failure effects of Control System technologies.

The Power Station, under the auspices of C&I Maintenance and C&I Engineering is accountable for the Management of Plant Software, and 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 is aimed at presenting minimum requirements effective 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 intent of the requirements is 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.

3.1.1 A First Step in meeting Requirements

The first step in meeting the Management of Plant Software Standard is to perform an assessment of 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, processes and validating these processes to ensure its proper functioning.

The assessment shall consist of the following:

1. The software system assessment shall be recorded in a register, and clearly documented.
2. Identifying the level of critical importance of control systems and assessing how long the plant can operate without the control system running. Within power plants, there are many control systems, some controlling highly sensitive processes, such as boilers and turbines critical to power plant operations. Similarly, there are less critical processes which can afford lower recovery importance. Therefore a detailed assessment of control system criticality shall be performed defining the need for software management and the manner in which 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 it is important that the methodology for managing Plant Software at the Power Station is compiled and effectively performed. This responsibility resides with the Power Station, who is 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 clearly 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 effective communicated.
4. Specific System-Back-Up and Restoration Procedures shall be kept to control 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 accessable 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.

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 Back-up 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 in the restoration of the control system functionality, and shall ensure that operations are normalised within a minimum time frame. The plan shall therefore identify vulnerabilities and recommend necessary control measures in the DRPs to address facilitate system recovery.

3.1.4 Software Inventory

A comprehensive inventory list of all Control Systems Plant Software shall be kept, managed and updated as and when software is modified, new Control Systems are added and keeping 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:
    I. Instrument Calibration Software Tools (such as HART).
    II. Instrument Setting Lists.
    III. Instrument programming tool software, programming units (PG's) and Laptops use 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

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 include, but is not only limited to these are:
    1. Unitized PLC/DCS and SCADA Software.
    2. Common Plant Systems Software.
    3. Automation and Application Server Software.
    4. Software used to perform Maintenance/Engineering functions.
    5. Systemd databases and system restoration files.
8. Accompanied with this, a detailed Risk Assessment of Plant Software should be kept, highlighting the risk which 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 maintain a current and functional Back-Up or Archive of Plant Software of all systems on a regular basis. It is recommended that incremental backups 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 Back-up or Archive Plan. The Back-Up or Archive Plan shall as a minimum describe;

1. The frequency of the Back-Up. Ensure that all files, Software, including system files, images are backed up regularly, on a systematic basis (which includes full and incremental backups).
    i) Full Backups – 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 optimize backup storage.
    ii) Incremental Backups – Incremental backups store only newly created or updated data since the last backup operation. This saves storage media space in contrast to full backups.
    iii) The methodology for system backup is to follow a Full Backup + Incremental Backup approach to systems (Figure 2).

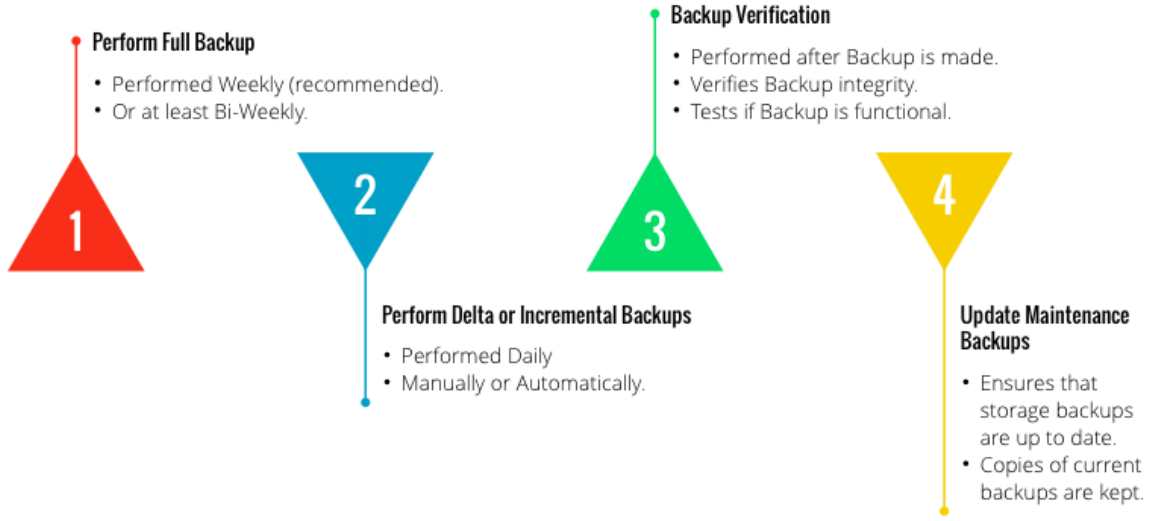

Figure 2 – Software Backup Strategy

2. Backup the entire system when making software changes, such as upgrades, modifications or major modification.
3. The process and functional requirements necessary for the creation of the Back-Up.
4. The process and procedures necessary for verifying the Back-Up.
5. The validity period of the Back-Up, from the time of Back-Up creation, after which, a new Back-Up of the Control System needs to be made.
6. The method of physical storage of the Back-Up. This shall include elements of Back-Up Storage Locations, Number of Back-Up Copies and Back-Up environmental requirements.
7. Testing of Back-Up shall also be performed and this is to be documented within the Back-Up Plan. (See Recovery Plans for additional Requirements).
8. Software backups 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 are aimed at improving the functionality and stability of the Control Systems and more recently, have been focused to enhance the security of the Control Systems technology. However, since patches can impact on 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 in accordance with 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 software versions, current and up to date.
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 maintained 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.

3.1.7 Checking / Verifying Updates and Backups

The Back-Up and Recovery Plans refers to the various strategies, and procedures required to protect and to recover from the Control System failures, and when this is required, it is essential that the Back-Up be fully functional and current for the operational application. Therefore, to ensure that the process of recovery is successful, it is necessary l for the Procedures and Back-Up'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 Back-Up and Restoration processes and procedures to ensure that Back-Up integrity is maintained. The following shall be carefully considering during Checking and Verification;

1. A Checking / Verification Plan shall be maintained and shall ensure fast recovery of failed Control Systems, and shall be thoroughly tested.
2. The integrity of the Plant Software on Back-Up shall be routinely tested through the application of 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 backups differ from the Plant Software used on the plant to such an extent that it cannot be easily modified to work on the plant any more, 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 specific 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 of the control systems. These sets (or copies) are updated at certain intervals. Backed-Up copies are updated regularly, after full backups 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 process of backup verification confirms that the backup procedures are current and functional.
    b. Secondly, backup verification ensures that the backup is functional, and that problems in backup procedure can be identified, understood and any "bugs" identified and corrected.
    c. The backup verification process facilities 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.

d. The backup verification process also consists of confirm 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 decided on by the system engineer.
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 both 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 to 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

The Storage of Plant Software and its methods should be in accordance with OEM recommendations and best practises, and 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 data life of the storage medium.

As a minimum, 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 difference locations. In some cases control system Plant Software, backups 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 are 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 which may occur.
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 is essentially aimed at preventing and detecting unauthorised changes or modification to Plant Software, and also to be aligned 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 responsibility of the control system administrator (or all personnel), who manage plant software shall be regularly reviewed and confirmed. In cases where the personnel who manages plant software is no longer an employee or a responsible person for Plant Software, his/her roles relating to software management shall be removed and the document to that effect updated at the applicable manager (C&I Engineering and or C&I Maintenance Manager). This includes the management of Plant Software during the construction projects.

Therefore, as a minimum, the following forms 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 l). 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 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 in the recovery of 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 last update, serial numbers, licensing and OEM contact information, and 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 to have 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 acceptsthat software changes are driven from the modification process. 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 plant performance has been proven.

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

3.1.11 Communication and Informing users

All users of the software 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 to assist in recovering a licence. A process should also be set up to specifically cater for the event of a licence loss. Hardware copies of licences (if it exists) should be kept to prove 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 the loading of un-controlled software on to 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, and this is especially enhanced by experienced System Administration, and by fulfilling the functions contained as 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 standardwhen 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.

3.1.15.2 Medium-term requirements

a. Implement this standard and associated site specific procedures and control software changes in such a way 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 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 on a regular basis, six monthly.

e. Dedicated plant maintenance procedures with regards to Plant Control System Software Management based on the requirements of this standard shall be compiled and registered for the required 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 of the relevant programming units or other engineering tools.

c. Log all changes to software in such a fashion that the changes will be apparent to everyone.

d. Update the maintenance copies regularly and after any changes.

e. Ensure compliance with this standard at all times.

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 failure of the system. Records and registers shall be kept on an archived Server.

Records must be kept until the plant is decommissioned, or until the current installed application has been fully replaced with a new system with its own software.

4. AUTHORISATION

This document has been seen and accepted by:

Name	Designation
Andre Van Den Berg	Senior Engineer: C&I Plant CoE
Andrew Botshe	Manager: C&I (Generation)
Christoph Kohlmeyer	Chief Engineer: C&I Plant CoE
Cornelius Visagie	Chief Technologist: PEIC C&I
Eugene Motsoatsoe	Manager: C&I Plant CoE
Jorge Nunes	Chief Engineer: PEIC C&I
Khaya Sobuwa	Middle Manager: C&I Plant CoE
Nerino Baruffa	Senior Consultant: PEIC C&I
Paul Du Plessis	Chief Technologist: PEIC C&I
Prudence Madiba	Senior Manager: EC&I CoE
Zubair Moola	Chief Engineer: C&I Plant CoE

5. REVISIONS

Date	Rev.	Compiler	Remarks
November 2012	A	Mr. John Viljoen	Draft Document for review created from 36-194 for TDAC
September 2016	0	Dr. Craig D. Boesack	Added additional paragraphs and content final Draft
January 2017	0.1	Dr. Craig D. Boesack	Final Draft for Comments Review Process
February 2017	0.2	Dr. Craig D. Boesack	Final Updated Draft after Comments Review Process
February 2017	1	Dr. Craig D. Boesack	Final Document for Authorisation and Publication

6. DEVELOPMENT TEAM

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

- Dr. Craig D. Boesack

7. ACKNOWLEDGEMENTS

- Jorge Nunes
- Corneluis Visagie

Appendix 1 – Minimum Documentation Requirements

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

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