PERCIPIENT & VERSIC FUNCTIONAL SAFETY MANUAL

Percipient Version 2.34 and above
VersIC Version 1.10.37 and above

1 Table of Contents

2 Revision History

Revision	Notes	Date
1.0	Initial Draft	2/26/20
1.1	Integrated feedback from Review v1.0c	3/17/20
1.2	Integrated VersIC Safety Manual	3/23/20
1.3	Updated Primary Assumptions of Use; added numbered headings	4/7/20
1.4	Updated Documentation Links	7/6/20

3 Document Purpose and Scope

This Functional Safety Manual discusses configuration, operation and use of Percipient IP Lifecycle Management and VersIC Design Data Management tools in the context of a safety-related system. It is intended to support IT System Administrators, IP Designers and Functional Safety Managers in using Percipient and VersIC in an ISO 26262 compliant way. To this end, the Functional Safety Manual both provides functional safety-related use instructions as well as describes relevant features and additional failure prevention and detection features provided by the tool.
The Functional Safety Manual provides a set of requirements and recommended best practices as well as a summary of tools failure modes for ensuring safety standards compliance of IP components and design elements, in a context of a Functional Safety-compliant application. The document also summarized use cases, relevant assumptions and data protection measures.

4 Tool Certification

Percipient, VersIC and this Functional Safety Manual have been evaluated by an accredited, independent third party to ensure compliance with relevant requirements of ISO 26262:2018. Based on these evaluation results, the tool was certified by the third party to have a predetermined TCL 1 per ISO 26262-8, Clause 11.

5 Tool Versions

This Safety Manual applies to Percipient Version 2.34 and above; and VersIC versions 1.10.37 and above.

6 Assumptions of Use and Customer Responsibilities

6.1.1 Primary Assumptions of Use

- In the context of Functional Safety, customer is responsible for ensuring that Percipient and VersIC are used as part of an ISO-26262 compliant design and development process. Usage of Percipient and VersIC tools alone does not guarantee ISO-26262 standards compliance. While Percipient and VersIC tools are essential in facilitating and managing complex and distributed IP development, and consequently supports the achievement of design goals, it does not automate or replace any of the safety activities and supporting processes required by ISO 26262:2018.
- Particular attention is drawn to ISO 26262-8, clause 11.4.2: As the confidence level evaluation of Percipient and VersIC was performed independently from the development of a particular safety-related item or element, the validity of this predetermined Tool Confidence Level shall be verified prior to their use in the development of a particular item or element.

6.1.2 Additional Assumptions of Use

- Tool installation and setup are performed correctly, in accordance to documented installation instructions.
- Recommended minimum infrastructure requirements have been met in accordance to Percipient and VersIC Administrator Guides.
- Tool has adequate disk space for storing IP design data and associated metadata.
- User permissions are set up correctly and maintained appropriately.
- Tool installation is connected to a data management tool, such as Perforce, which is the primary storage for IP design data.

Note that if some or all of above requirements are not met, tool use may result in failure, as documented in Summary of External Tool Failure Causes section of this document.

7 Percipient

7.1 Tool Description

Percipient is Methodics' comprehensive IP Lifecycle Management (IPLM) platform, enabling companies of all sizes to have complete control over the design and integration of both internal and external design elements including libraries, new analog and digital design, and standalone IP.

Percipient maximizes internal and external design traceability and reuse by tightly coupling IP creators with IP consumers. Centralized cataloging, automated notifications, extendible permissions, and integrated analytics provide the transparency and control needed to streamline collaboration. Percipient's unique IP/block-centric approach to management ensures everything from design creation through to defect tracking is associated with the design hierarchy.

7.2 Tool Use Case Summary

The following list summarizes most common use cases of Percipient tool.

1. User, Group and Permission management. Protecting security of IP is an essential capability of Percipient for enabling ISO26262 standards compliance. IP designers can add, edit and remove users and groups. IP permissions such as Owner, Write or Read can be assigned to both users and groups, providing granular control over what types of tasks individual groups and users can perform. Users and groups can also be enabled and disabled Percipient as an additional security measure.
2. Library and IP metadata management. Percipient's IP metadata management is a core capability that enables traceability and reuse of IP data. IP designers can create and update IP Libraries as a way to organize related IPs. An IP Library contains one or more IPs, which represent IP design components. Both IPs and Libraries can include a variety of metadata, such as Properties, Property Sets and Attributes. User can add new IPs and associated metadata, edit and delete existing IPs and metadata. Additionally, users can add and modify Resource IPs as a way to build a hierarchical BoM IP.
3. IP Version management. Users with correctly set up permissions are able to create new versions of IPs based on changes on metadata, addition and removal of resources or to IP design data itself. Related functionality include ability to compare different versions of IPs and review hierarchical IP structures; review usage of an IP Version as a Resource of other IPs; assignment of static or moving aliases to IP Versions
4. Workspace management. This use case includes capabilities for creating an IP designer workspace and populating the workspace with design data for a specific IP hierarchy – which includes the top level IP as well as the IP's resources. When another user creates a new IP Version, other users can be pick up the changes by updating their workspace to a latest or a specific version of an IP.
5. Cache management. Users can set resource IP to either "local" or "refer" mode in order to manage their disk space usage. IPs in "refer" mode reside in IP cache. Users can also publish

IP changes into the cache directly so that other users can automatically use the cached data in their workspaces.

7.3 Summary of Fault Detection

Percipient provides several methods for fault detection, including fully automated fault detection and rollback mechanisms.

1. Most operations in Percipient support atomic transactions. When an operation partially fails due to connectivity issue or other external condition, the transaction handler automatically detects the failure at the database level. The entire transaction is then automatically cancelled, and partially updated data is rolled back to its original state.
2. In some cases, Percipient relies on external systems to complete an operation. For example, in the case of creating an IP workspace, Percipient relies on underlying data management system such as Perforce to load the IP design data. If the DM data transfer operation fails, the error condition is intercepted by Percipient and the rest of the operation is then cancelled. In this scenario a partially completed operation is possible resulting in a corrupted user workspace.

7.4 Tool Classification Summary

Below table is a summary of tool classifications. A detailed analysis can be available upon customer request.

Use Cases	Malfunction	TI	Effect on output and element	TD	Detection / Protection Measures	TCL
1, 2	Non-IP metadata update operation fails due to system failure.	1	No effect	N/A	N/A	1
1	User access revocation failure due to system failure.	2	User retains unauthorized access to IP data and is able to make unauthorized changes	1	Functional failure is reported to administrator so that the command can be attempted again. Failure also reported via Events system as well as logged. See References section below for Administrator's Guide for additional details on error log configuration. Customers must follow ISO- 26262 compliant processes to ensure full FuSa compliance. In particular review and other V&V, version control, configuration management, and functional safety audit.	1
2	Update or delete IP metadata operation fails due to system failure.	2	IP output or element contains undesired data, leading to incorrect behavior.	1	Functional failure is reported to administrator so that the command can be attempted again. Failure also reported via Events system as well as logged. See References section below for Administrator's Guide for additional details on error log configuration. Customers must follow ISO-26262 compliant processes to ensure full FuSa compliance. In particular review and other V&V, version control, configuration management, and functional safety audit.	1
2	View IP metadata operation fails due to system failure	1	No effect	N/A	N/A	1
4,5	Create workspace operation fails or partially succeeds due to system failure	1	No effect on IP data, workspace is unusable	N/A	N/A	1

3	Create IP Version fails due to system failure	1	Workspace contains outdated / incorrect or inconsistent data, leading to inaccurate view of IP data, which can result in undesired new changes	1	Functional failure is reported to administrator so that the command can be attempted again. Failure also reported via Events system as well as logged. See References section below for Administrator's Guide for additional details on error log configuration. Customers must follow ISO-26262 compliant processes to ensure full FuSa compliance. In particular review and other V&V, version control, configuration management, and functional safety audit.	1

7.5 Data Integrity

Percipient tool ensures data integrity of internal data using the following set of mechanisms.

7.5.1 Neo4j Transactions

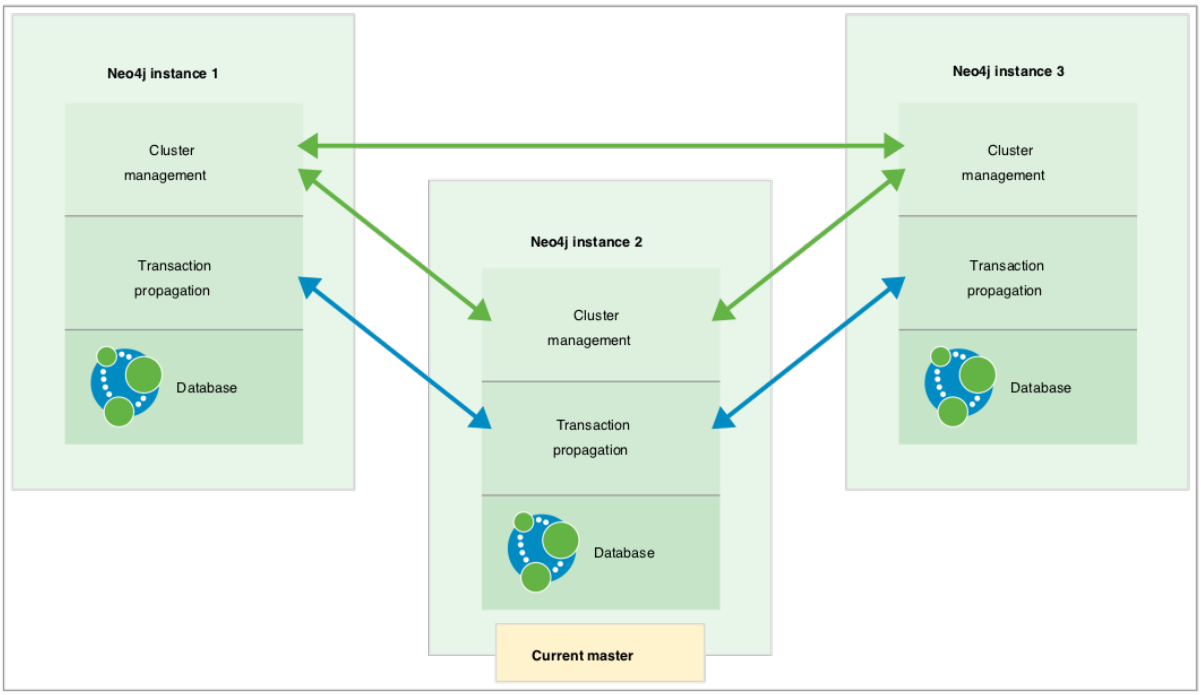
Percipient's underlying data storage technology is based on Neo4j database. Data integrity is provided via Neo4j's Transactions mechanism. In order to fully maintain data integrity and ensure good transactional behavior, Neo4j supports the ACID properties:

- atomicity: If any part of a transaction fails, the database state is left unchanged.
- consistency: Any transaction will leave the database in a consistent state.
- isolation: During a transaction, modified data cannot be accessed by other operations.
- durability: The DBMS can always recover the results of a committed transaction.

When an operation fails or partially succeeds, the data is rolled back to its original state, preventing data corruption in case of system failures during data write operation.

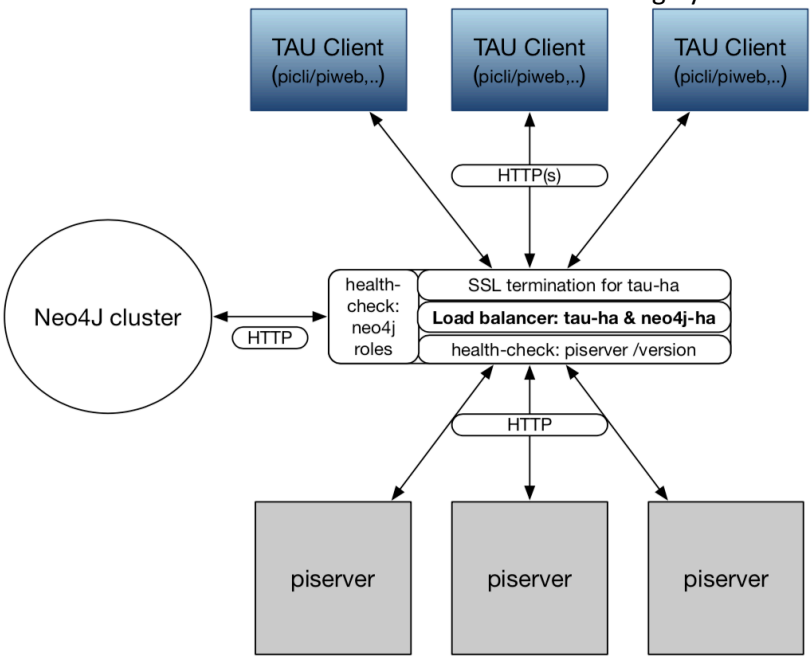
7.5.2 Redundancy and HA Architecture

Percipient is designed to operate in a High Availability configuration, which provides internal redundancy of components. At the database level, data storage redundancy is provided by Neo4j HA Cluster Architecture



In this configuration, data is written to Master instance and is replicated to one or more Slave instances. The replication happens in a transactional operation, so that a replication failure will not result in any data corruption on the Slaves. In case of Master instance becomes unavailable, the cluster automatically fails over to one of the Slave instances, which are then promoted to a Master.

Percipient's CLI, PiWeb and PiServer components are also set up in an HA configuration, ensuring that connection between user and database remains highly available.



See HA Deployment and Configuration in References section of this document for more detailed information.

8 VersIC

8.1 Tool Description

VersIC is a Design Data Management tool for IC Designers and provides a unified interface to modern software configuration management (SCM) tools for Cadence's Design Framework. Fully integrated auto-checkouts/checkins are enabled without any back-end database user knowledge required, Cadence simulation methodologies are fully supported and release methodologies utilizing sophisticated SCM techniques can be employed in an IC Design context. VersIC supports Subversion and Perforce SCM tools.

8.2 Tool Use Case Summary

The following list summarizes most common use cases of VersIC.

1. Check in and Check out. Managing design data stored in SCM systems like Perforce from within the Cadence design environment is a key capability VersIC provides to make SCM functionality available to designers. Files can be checked out, modified, and checked back in using native Cadence data structures to group the managed files. Automation of the management of ancillary Cadence database files is provided to simplify user workflows.
2. Managed Data Comparison. A key function of VersIC is the ability to compare current or past versions of Cadence design data to other versions of the same or different data. Users can select which data to compare, and VersIC provides a detailed analysis of the difference between the data, inside the user design environment.
3. Workspace Update Management. Users can control when and how modifications from other users are brought into their workspace. VersIC notifies users when updates are available, and users can bring in the desired changes in order to efficiently integrate their design.

8.3 Summary of Fault Detection

VersIC provides fault detection based on mechanisms provided by host application such as Cadence Virtuoso as well as underlying Data Management system, such as Perforce.

8.4 Tool Classification Summary

Below table is a summary of tool classifications. A detailed analysis can be available upon customer request.

Use Cases	Malfunction	TI	Effect on output and element	TD	Detection / Protection Measures	TCL
1, 2, 3	Malfunctions related to failures of underlying data management systems, such as Perforce or Subversion.	2	IP data does not contain required changes	1	DM operation is cancelled and resulting DM error message is returned to the user. User can take corrective action based on the error message. Customers must follow ISO-26262 compliant processes to ensure full FuSa compliance. In particular: review and other V&V, version control, configuration management, and functional safety audit.	1
1	Check In or Check out failures of underlying data management systems, such as Perforce or Subversion.	2	IP data does not contain required changes	1	DM operation is cancelled and resulting DM error message is returned to the user. User can take corrective action based on the error message. Customers must follow ISO-26262 compliant processes to ensure full FuSa compliance. In particular:	1

					review and other V&V, version control, configuration management, and functional safety audit.	
2	Managed Data Comparison fails due to system failure	2	User is unable to verify current design compared to past versions; design may not contain required changes	1	Functional failure is reported to the user as an error message. Customers must follow ISO-26262 compliant processes to ensure full FuSa compliance. In particular: review and other V&V, version control, configuration management, and functional safety audit	1
3	Workspace update fails due to system failure	2	Workspace does not contain required data.	1	Failure is reported to user, so update can be attempted again. Failure is logged. Customers must follow ISO-26262 compliant processes to ensure full FuSa compliance. In particular: review and other V&V, version control, configuration management, and functional safety audit	1

9 Summary of External Tool Failure Causes

The most common causes of tool failure are due to the following anomalous conditions. These failures can occur when tool is not properly configured as documented in Assumptions of Use section of this document.

9.1 Infrastructure Failure

Infrastructure failure is a common cause for tool failure. This can include network issues, which is the most common type of issues, hardware failure or similar types of issues. Specifically, for network-related issues, Percipient is typically deployed in a High Availability configuration (see HA Deployment and Configuration in References section), which provides significant protections for issues related to individual server failures, and limited protection for network related issues. For example, if Percipient authentication is configured to use external LDAP authentication and the network connection between Percipient and LDAP becomes unavailable, users will not be able to log into Percipient for the duration of the outage. Some types of infrastructure failure can lead to tool outage even if configured in High Availability deployment. For example, if the Neo4j database cluster is deployed on a single switch, that switch can become a single point of failure, which can lead to tool outage in case of the switch failure. Methodics recommends for customers that High Availability configuration is deployed with ensuring that each redundant component shares minimal or no infrastructure with other components.

9.2 Incorrect Configuration

Incorrect tool configuration can lead to failures. Tool Administrators must ensure that setup instructions are correctly followed. An example of this type of failure can include failure to properly configure connection between a DM system such as Perforce and Percipient. The tool heavily relies on the underlying Data Management system, and many critical features will not work if the connection is misconfigured. Methodics provides detailed setup instructions for external system dependencies. See External DM System Configuration in References section for more details.

9.3 Insufficient Resources

Insufficient system resources may lead to failures in cases when minimal requirements for infrastructure have not been satisfied, or when load on the tool exceeds available resources.

Customers must estimate required resources, such as disk space needs, CPU and memory allocation that would be sufficient to sustain user's needs. Methodics provides customized infrastructure recommendations specific to customers individual needs. See Percipient Hardware Recommendations in References section.
When the tool encounters insufficient resources, some functionality may result in unexpected errors or slow response time. For example, the database does not have sufficient disk space to store IP metadata, any write operations will result in failures and block users' ability to update IP design data.

10 References

List of Methodics resources related to this Safety Manual.

- Percipient Administrator Guide. https://docs.methodics.com/display/PER/Percipient+Administration+Manual
- External DM System Configuration. https://docs.methodics.com/display/PI2/Perforce+Configuration
- Percipient Hardware Recommendations. https://docs.methodics.com/display/PI2/Methodics+Hardware+Recommendations
- HA Deployment and Configuration. https://docs.methodics.com/display/PI2/HA+Deployment
- Percipient User Guide. https://docs.methodics.com/display/PER/Percipient+User+Guide
- Percipient Tutorial. https://docs.methodics.com/display/PER/Percipient+Training
- Perforce and Percipient Configuration. https://docs.methodics.com/display/PI2/Perforce+Configuration
- IP Design Workflows. https://docs.methodics.com/display/PI2/Workflow+Discussions