



**FDA 21 CFR Part 11
zenon in Regulated Industries**

Executive summary

The Part 11 regulations concern all electronic systems which create, modify, maintain, archive, retrieve or distribute data concerned with regulatory safety. They establish the acceptance criteria for the use of electronic records and signatures, under which they will be considered equivalent to conventional paper records & handwritten signatures.

COPA-DATA and its zenon Product Family provide solutions that ensure safety and security in FDA regulated environments. A strict internal company Quality Management System provides transparent development procedures ensuring a product family of high quality and reliability. We aim to provide solutions which not only adhere to the Part 11 regulations, but provide the most efficient platform to develop regulated projects, giving efficient engineered solutions reducing the validation effort needed. This document describes the FDA 21 CFR Part 11 regulations, and how zenon is in full accordance with the regulations, promoting innovation through validation efficient development.

zenon makes validation as efficient as possible.

Communication:

The zenon system includes native communication drivers which interface directly with the connected hardware and systems, no configuration on the 3rd party system is needed, zenon simply connects with full duplex data exchange. The interface is integral to the zenon design environment and so validation is reduced to qualifying the zenon project. In this manner 'Read only' connections to 3rd party validated systems will not affect the validation status of that machine. The communication drivers extends vertically to MES, ERP, Database, and IT networks, providing the same efficient environment with strong links to business and operations.

Parameters instead of programming:

zenon has extensive functionality at the click of a mouse. Setting parameters in place of programming has strong benefits in regulated environments, it reduces risk, novelty, and complexity. The ISPE GAMP guidelines classify such products as 'Software category 4' which dictate a much reduced validation model.

Integral functionality:

The library of functionality contained in zenon allows for the full scope of production automation projects to be realized utilizing the parameterization in place of programming. FDA 21 CFR Part 11 compliance is therefore possible in all projects and is made as efficient as possible. Efficient engineering being applied to GMP environment has the added effect of efficient validation & qualification.

Flexibility:

zenon is modular and scalable, utilizing the above integral functionality opens up opportunities that provide innovation and optimization in integrated or standalone systems. A strong communication platform benefits legacy installations by connecting to existing equipment and systems. New installations benefit with unrestricted choice of control hardware and systems.

Part 11:

Configurable systems reduce significantly the validation effort associated with automation in GMP environments, adhering to the regulations with a suit of technology focusing on Electronic Records and Signatures, Archiving, and Security. Having a configurable system with integral functionality, a strong communication platform, and strong visualization, makes any project a FDA compliant project. We reduce validation and qualification by applying the ISPE GAMP guidelines to reduce risk, novelty, and complexity.

From Recipe or Batch instruction and throughout the production operation, the process is monitored and recorded from several angles provided by zenon's audit-trail, alarms lists, and archives, giving live analysis and concluding with defined production and quality reports. The divide at which you define the collation of GMP relevant data is under the users discretion, with multiple possibilities to integrate to others system or operate as a standalone system generating all GMP data.

zenon offers fully redundant systems, ensuring data security and maximum availability.

'Out Of The Box' GMP, all functionality is contained in one product to provide GMP projects with the required security and functionality to ensure compliance to the Part 11 regulations.

zenon operates as a secured closed system, where all required functionality requires a user to login with two credentials, a User Identification and a Password. External systems which provide user access security such as biometric access control can be implemented into the zenon security system. Each user can be administered locally in the zenon User Administration and/or integrating into a wider user management system through Windows Active Directory.

zenon Pharma Edition is built on the proven foundation of zenon, focusing on the management of regulated projects and the streamlining of validation.

zenon Pharma Edition provides enhanced functionality which embraces the unique environment of pharmaceutical projects and their life-cycle from concept to retirement. Each regulated company has a unique structure and workflow to achieve their model of Part 11 compliance. zenon Pharma Edition effectively manages regulated projects and their life-cycle, which positively impacts on the validation effort needed, and reduces the associated risk of regulated projects.

zenon is a complete family of products aligned with the Pharmaceutical and Life-Science industry challenges, in operation, design, and innovation.

Contents

zenon in Regulated Industries	1
Executive summary	2
Contents	4
1. Introduction	5
2. FDA 21 CFR Part 11 regulations	5
Subpart A—General Provisions.....	5
3. Part 11 compliance with zenon	7
Business benefits of zenon in FDA environments	8
4. Wider scope of compliance	9
GAMP software category 4, Parameterization	9
Integral functionality	10
Communication	11
Vertical integration	12
Redundancy.....	12
Modules and functionality	12
Backward compatibility	21
Project Versioning & Backup capability	21
History of changes	22
Distributed Engineering	22
5. zenon Pharma Edition	23
Pharma Wizard	23
Documentation wizard	25
Comparison wizard	25
In combination	26
6. COPA-DATA quality management	27
Product development management.....	27
Human Resource Management.....	27
External audits	27
7. Part 11 compliance table	28
Subpart B—Electronic Records	28
Subpart C—Electronic Signatures	36

1. Introduction

This document provides the details and information on how zenon is in full accordance with the FDA 21 CFR Part 11 regulations.

The FDA 21 CFR Part 11 regulations (hereby referenced as 'Part 11 regulations') establish the acceptance criteria for the use of electronic records and signatures. Under which they will be considered equivalent to conventional paper records & handwritten signatures.

Such electronic systems employ procedures and controls designed to ensure the authenticity, security, and confidentiality of electronic records.

The Part 11 regulations concern all electronic systems which create, modify, maintain, archive, retrieve or distribute data concerned with regulatory safety.

Software products such as zenon cannot be certified or validated themselves, it is the end process which is validated. However the software needs to offer functionalities, workflows, and security that enable the customer to create validated projects.

2. FDA 21 CFR Part 11 regulations

The Part 11 regulations are separated into three sections. Firstly 'Subpart A' gives the general scope of the regulations, with a description of its definitions, and introduces what is covered in greater detail in the following two sections. The detailed criteria is laid out for Electronic Records in 'Subpart B', and for Electronic Signatures in 'Subpart C'. This document holds a 'Part 11 Compliance table' where Sections 'B' & 'C' are listed in detail, the Part 11 regulation requirements are displayed with a statement of how this is satisfied in zenon.

The text below is an extract from 'Subpart A' of the Part 11 regulations. 'Subpart B' and 'Subpart C' of the Part 11 regulations are described later in the 'Part 11 Compliance table' chapter.

Subpart A—General Provisions

§ 11.1 Scope

(a) The regulations set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under

requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full hand-written signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

§ 11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the in-tended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§ 11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other de-vices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

3. Part 11 compliance with zenon

For automated projects operating in regulated areas, having functionality to comply with the Part 11 regulations is required without exception.

zenon embraces fully the demands of these regulated environments, with Audit-Trail, Alarm management, User Administration, Security, Archiving, and Reporting, in one system allowing for standalone Part 11 compliance, or as a part of an integrated system and its Part 11 compliance.

With zenon all projects are capable of Part 11 compliance. The philosophy of zenon is parameterization instead of programming, utilizing a 'Use by many library' covering the full scope of functionality to provide automation, HMI, and SCADA operation functionalities. Parameters are simply set to enable the required functionality and in the required manner specified under the Part 11 regulations.

Having a parameterized system which has the full integral functionality and native communication to industrial systems and networks, means that validation can be made

as efficient as possible. Native communication means that connection to systems and networks is achieved without the need for another system to be involved, therefore validation is only concerned with the zenon project, and not the interface, as the interface is integral to the zenon project. Also the fact that native communication is used no design or configuration on the 3rd party system is needed, zenon simply connects with full duplex data exchange. Integral functionality and parameters in places of programming, allow full control over the full scope of the project, in this manner risk is reduced as the software is simply configured, the parameters cover the full scope of the project and its behaviour, Part 11 compliance is therefore entirely possible in all projects at any phase of the development.

Quality is designed into a system from the beginning, in this regard zenon has been developed from the outset to accommodate GMP (Good Manufacturing Practice) regulated environments such as outlined in Part 11 and other international regulations. This inherent design is integral across the zenon design environment, enabling this behaviour and functionality to suit individual needs is achieved through simple configuration of the individual modules and components.

Business benefits of zenon in FDA environments

Setting parameters instead of programming provides a configurable system. Being classified in the ISPE GAMP guidelines as a 'Software category 4' product, reduces risk, novelty, and complexity. All of which has a positive effect on the validation effort, reducing the cost associated with automated projects.

The philosophy of COPA-DATA is efficient engineering, in that complicated functionality should be designed into the product leaving the designer simple parameters which utilizes the pre-defined functionality. This follows the ideal of 'Quality by Design' where proven and tested functionality forms the library for development.

One stop automation product. zenon provides a suit of functionality, from production request using zenon's ISA 88 Batch Control or our Recipe management, through production monitored and recorded by audit-trail, alarm management, historian archives, giving live analysis and concluding with a production batch report.

zenon simply connects. A strong communication platform of native drivers interfacing directly to control systems and hardware without external interfaces to design. Efficient communication which reduces cost through low engineering and implementation effort. Fast efficient networking brings systems together, which are independent of hardware manufacturer, and provide easy integration of new and existing legacy systems. Connection to validated systems in a read only mode can be established without changing the validation status of the connected equipment.

All product research and development is conducted within COPA-DATA. All products are traceable in a quality management system employing strict procedures throughout their development & operational life-cycle.

With a strong communication platform, integral functionality, which is enabled through configuration, adds up to an effective automation system for regulated environments. Providing out of the box GMP functionality with Part 11 compliance at a mouse click, creates an efficient validation environment where any project can be Part 11 compliant.

Certification with other connected products and systems offers the assurance that zenon has been successfully tested with these systems, and that security of data is enforced.

Microsoft Gold Certified Partner. COPA-DATA is a 'Gold Independent Software Vendor (ISV)' signifying our commitment to design software products unified with the Windows Operating system, this enables the complete acceptance and use of the security features of Windows. zenon supports all windows platforms, which are interchangeable on the same project.

SAP certified interface. The zenon ERP interface was certified by SAP, making it possible for you to seamlessly integrate your production and business applications.

OPC UA certified server, COPA-DATA is a member of the OPC foundation and has a certified OPC server, which provides consistent and secure transfer of data for robust reliable network communication. The OPC server has a well developed security concept which protects all data from unauthorized access.

4. Wider scope of compliance

Functionality to achieve Part 11 compliance is only one part of the challenge. How this functionality integrates into other connected systems & processes is a further challenge zenon embraces and provides efficient and effective solutions.

As production equipment and processes evolve, a flexible approach to system design is needed to provide leading technology and innovation. Having a static system with pre-described non-flexible solutions can have severe implications on the outcome of a system and the possibilities such a system is capable of. zenon has a very flexible approach, which is able to provide innovation and through integrated functionality keeps the validation effort to a minimum. This approach opens up opportunities that fit to existing installations, new equipment and facilities, or to define the ideal Quality Management for a given unique production facility.

GAMP software category 4, Parameterization

zenon is a configurable product using parameterization instead of programming, therefore correctly administered zenon solutions can be classified as 'GAMP software category 4'. As this reduces Risk, Novelty and Complexity in the automation solution, zenon provides an efficient validation environment.

The philosophy of COPA-DATA is efficient engineering, in that complicated functionality should be designed into the product leaving the designer simple parameters which utilizes the pre-defined functionality. This has created a platform in which entire applications can and are developed using only parameterized zenon functionality. This holds great benefit as the 'Used by many library' which is fully tested and documented by COPA-DATA adheres to the GAMP software category 4 being a configurable product. Having an extensive and flexible library of functionality reduces the risk and novelty aspect of any project design under zenon, which has the desirable effect of reducing quality documentation as only the usage of the function and not the function itself needs to be qualified and tested.

zenon also comes equipped with VBA, C#, and VB.net capabilities which allow for bespoke and customized functionality, usage of which takes the functionality outside of the use by many library and GAMP software category 4. However these functions can then be designed once, validated, and used as a parameterized function within zenon. In this example the programmed code falls under the GAMP software category 5, and would need the required testing and qualification. But once this has taken place, the use of the function falls under the GAMP software category 4, as a configurable functionality. This flexibility allows full access to all zenon and bespoke functionality, and aims at providing easy engineering, reducing risk, and allowing generic quality documentation to be utilized across projects.

Each installation of zenon comes equipped with the full functionality already prepared for use in any project. The activation of each software module and function is carried out by the individual license. This has advantages to the effect that when future modifications of the project take place, the only change to the process is the project itself, no re-installation of zenon is necessary or addition of a patch, just a license key change and the changes to the project. Therefore in terms of qualification of the equipment, the scope of the project change is managed by the comparison and versioning in zenon, which can be documented and qualified. No change has been made to the system on which zenon runs, therefore the scope to the validation of the process remains at the level of the project change.

Integral functionality

zenon has a wide range of integral functionality offering the full scope of application utilizing its internal library, which is accessed via parameterization. Holding such functionality internally to all installations of zenon means that entire GMP projects can be implemented in one product, and if needed as a standalone project. The requirements for Audit-Trail, Alarm management, Archiving, Reporting, and Analysis, are all catered for in each zenon installation. The advantage this offers is that a full process can be realized in a standalone application, the integration of which can be applied in the most efficient way for quality and operation.



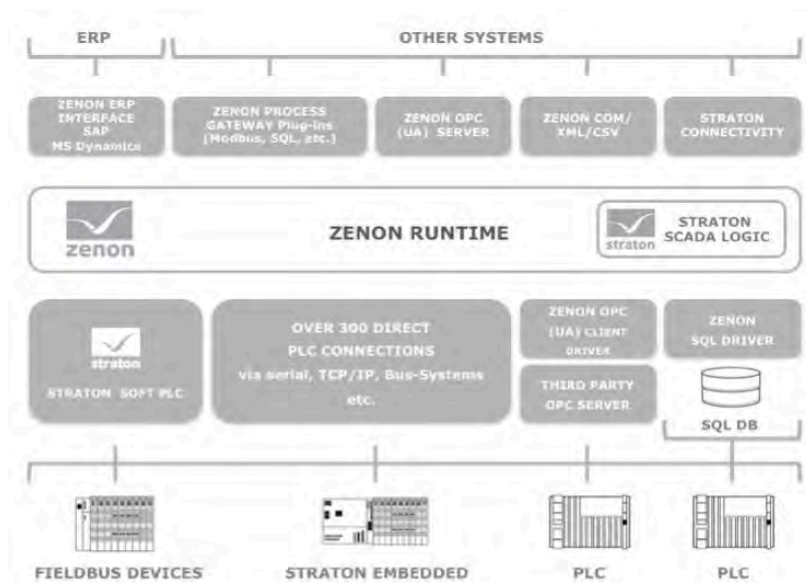
zenon's integral functions cover the full scope of production activities.

From Recipe or Batch instruction and throughout the production operation, the process is monitored and recorded from several angles provided by zenon's audit-trail, alarms lists, and archives, giving live analysis, and concluding with defined production and quality reports. The divide at which you define the collation of GMP relevant data is under the users discretion. The process and archived data can then be exported on command, automatically on event, or on a time basis. Providing the possibility to have a standalone system generating all GMP data, or as a part of a fully integrated system.

zenon has the benefit that each system can generate and hold its own GMP data, therefore in the event of a network failure for example, all production data is safe guarded and can be held locally. Then on restoration of the network and associated distributed systems, the required data can be exported. Therefore no production data has been lost, production can continue, and no risk to the product or process has been compromised, the production system continues without adverse effect.

Communication

zenon is an independent and flexible system. It can connect natively to different industrial systems, IT systems, devices, and networks. In this manner many different system can be effectively connected together. zenon's native drivers connect to these systems directly, and rely on no other system to provide this communication, and require no software or modification on the 3rd party system. Having the ability to connect to systems, devices, and networks, without making any changes means that connecting with zenon to the 3rd party system does not affect the validation of this system. If any control is then applied to the 3rd party system only this control needs to be validated, and there is no other connecting system in the process which would also need to be validated. If only data acquisition is required there would be no impact on the validation and quality documentation for the 3rd party system as no control changes or addition to this system have been made.



zenon can connect to different systems natively, bringing multiple systems together.

When a distributed communication system has been developed, not only the distributed application and its data storage needs to be validated, the interface between the systems also needs to be tested, documented, and qualified. As zenon has an extensive range of communication protocols this interface is no longer in the system, as zenon takes care of this internally.

Having native drivers to industrial networks and PLC's has the benefit of being independent of hardware manufacturer, providing easy integration of new and legacy systems, whilst reducing the complexity and risk. This environment brings multiple systems together. Such a reduction of engineering design and reduction of risk to the system, has significant positive effects on the quality and the level of validation needed.

Vertical integration

The communication model of zenon extends upwards to fully integrate into production MES and business ERP systems. zenon's strong communication platform includes all layers of a production environment and extends to these systems.

The discussed modules of zenon have the required functionality to interface to these systems. The Audit-Trail, Alarm message list, and Archives can all save and export their data into external systems, such as SQL database, XML files, CSV, dBase.

Bilateral communication can also be interfaced through specific communication drivers and gateways, such as: SAP, Microsoft Dynamics, SQL, OPC, Modbus.



zenon interface is certified by SAP

Redundancy

zenon has several methods for enabling redundant systems and operation.

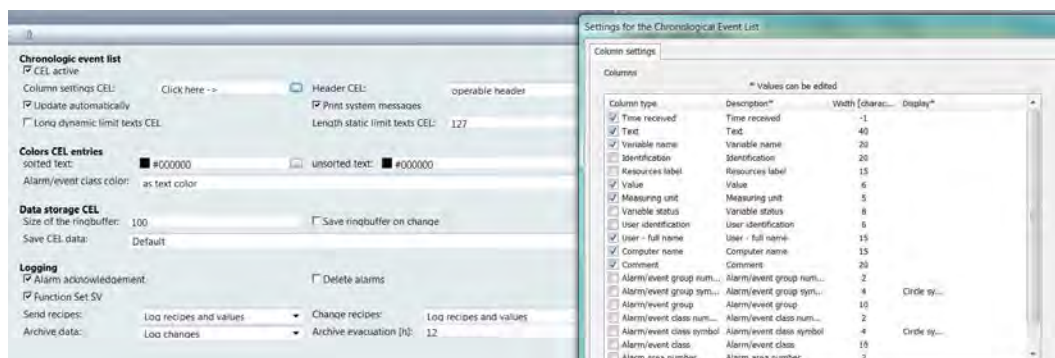
Classic redundancy with a duty and standby server enables secure systems with high data security and maximum availability.

Circular redundancy exploits the existing resources of multi-project installations. Where a neighbouring project simultaneously serves as a standby server in addition to its normal operation. Redundancy and security is obtained without additional hardware, therefore without additional cost and qualification.

Modules and functionality

Audit-Trail

Any event either by the system, connected systems, or operator intervention can be logged in the audit-trail. zenon's 'Audit-Trail' named Chronological Event List (CEL) records any variable or system event with time-stamp for the event, its acknowledgement, and when the event was resolved. Including the variable event name, its identification label, the full user name, user ID, system and project name, value (optionally with Old & New values), variable status, alarm text, alarm group & class, together with the possibility for a user to add a comment.



Configuration in the zenon editor of the audit-trail behaviour and detail.

Without fail all events can be monitored, and analyzed ensuring the protection and proof of production for regulated safety.

On user functions, the operator can be requested to login even if they are already logged into the system, the operator can also be requested for a comment to give a reason why this access is being requested, all is stored in the audit-trail providing electronic signature linked to the electronic record.

When downloading or changing recipes, the option exists of how much information is recorded in the audit trail. It can be set that only the recipe name is recorded in the audit trail, or all the variables that are downloaded or changed in the recipe are listed in the audit trail (optionally with Old & New values).

The 'Audit-Trail' is easily integrated into other systems, it can be exported to an external system via an automatic event, external request, timed event, or operator request. The data can be exported in several formats: dBase, CSV, XML, or directly to a SQL database.

Alarm Management

zenon has full alarm management functionality, any variable (user, process, or system) can apply multiple limits, these limits can then be classed as an alarm or warning with different alarm groups and alarm classes.

Reaction matrix
 Reaction matrix: <no reaction matrix linked>

Limit[1]
 Limit active (Delete limit): Click here ->

Limits[1]
 Limit text: Low Limit Reached
 Limit: 0.0 Minimum/Maximum: Maximum
 Threshold value: 0.000000 Delay time [s]: 0
 Dynamic limit active Variable: BatchProcess/Global/PrimaryReact

AML/CEL[1]
 In Alarm Message List In Chronological Event List
 To acknowledge Comment required
 To delete Print
 Alarm/event group: 0 - < not used >
 Alarm/event class: 0 - < not used >

Function[1]
 Function: < no function linked >
 Call via button in Alarm Message List

Additional attributes[1]
 Limit color: #FFFFFF
 Invisible Flashing
 Additional information 1:
 Additional information 2:

Help[1]
 Help file:
 Help chapter:

Alarm management configuration in the zenon editor of a particular variable.

Any number of limits can be defined for each variable. The value for each limit can be defined in multiple ways: a static value, a dynamic value set by another variable, or via a reaction matrix. Superfluous entries to the alarm list can be avoided by setting a hysteresis level to each variable, also a delay time can be applied where the alarm event must be active for a certain period before the alarm is generated.

A 'Reaction Matrix' supplies several decision and reporting capabilities for a single variable. Different events can be designed for this variable, with different alert text being communicated to the audit trail and alarm list. Functions can also be applied to this decision tree providing opportunities to define corrective action when violations are being approached. The status of a variable can also be monitored, displaying for example when a connection has been lost to a certain device.

Each limit has an associated text, which can be listed in the Alarm List and/or Audit-Trail (CEL). Each limit can force the user to add a comment for the violation, and can request an acknowledge before an alarm is resolved. Alarms can be attributed different groups and classes, allowing for hierarchies and segmentation to provide clarity. Individual colours can be applied to alarms to provide further distinction in the runtime screen and also the alarm list. To further instruct the operator for each alarm an individual help file can be opened at the relevant chapter, this aids the user and gives information of a procedure to follow when this event occurs.

Any limit can be configured to automatically trigger a function, this can execute any zenon function or user bespoke function. Which may include warning specific operators using the Message Control, taking aversive action by setting defined values, opening specific screens to guide operators, storing or exporting the alarm or audit-trail for detailed analysis of the event, or any other zenon function.

Analysis

zenon has a trending tool to aid the analysis of events and processes, this can be linked directly to Live values, Archives, Audit-Trail and Alarm management, to display and reconstruct with great detail events or occurrences that are or have previously occurred. This can provide the justification for proof of production when non-standard operations have taken place.



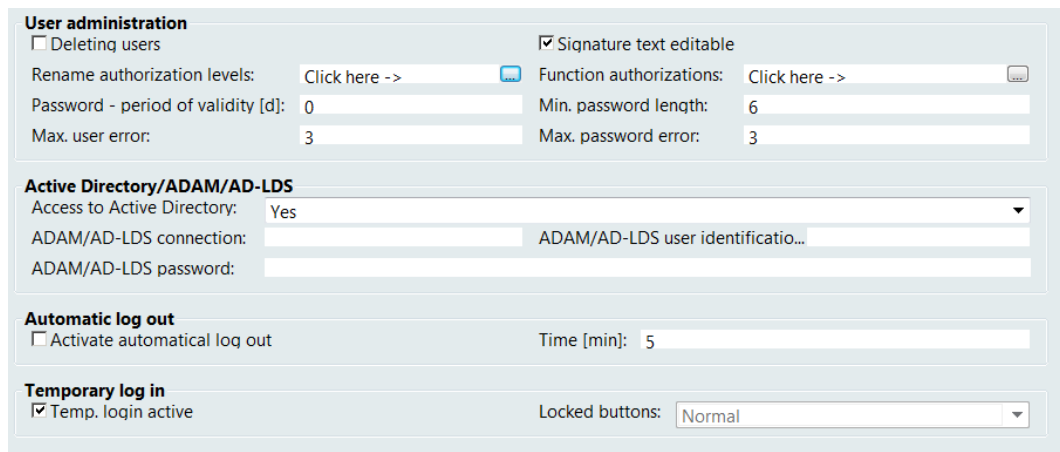
Examples of analysis capabilities showing GANTT, Trend, Alarm List and Audit-Trail.

Together with the reporting options (discussed later in this section) available in zenon, a complete analysis of the system can be accessed and recorded to be used as production and regulation transparency.

User Administration

zenon operates as a fully closed system, where all functionality including viewing screens, changing variables, acknowledging alarms, commenting on audit-trail events, starting, stopping, etc., requires a user to login with two credentials, a User Identification, and a Password. External systems which provide user access security such as biometric access control can be additionally implemented into the zenon security system.

zenon has two implementations of access control: a local user administration where users are assigned in either the zenon editor or in the run-time application, at least one Administrator is needed to provide the management of accounts, users can be enabled and disabled. The second method involves Microsoft Active Directory, where zenon's access control can be included into a wider user management system provided by the end users IT infrastructure.



User administration

Deleting users Signature text editable

Rename authorization levels: Function authorizations:

Password - period of validity [d]: Min. password length:

Max. user error: Max. password error:

Active Directory/ADAM/AD-LDS

Access to Active Directory:

ADAM/AD-LDS connection:

ADAM/AD-LDS password:

Automatic log out

Activate automatical log out Time [min]:

Temporary log in

Temp. login active Locked buttons:

Configure user authorizations, password behaviour, and Active Directory parameters.

Individual users are given specific authorization levels in which they can operate. User groups can be optionally defined where generic authorization levels are set, and each user is assigned relevant user groups. A user can be applied User Groups and specific Authorization levels, to create the required security needed by a each user of the system.

Password expiry can be enabled, forcing the user to change the password after a given period of time has elapsed. Any false login attempts are recorded, and the user or system is locked down in the event of false data being entered. If the password for a given user is violated more than the defined number of times, then the individual user is locked. If an invalid user name is entered more than the defined number of times, the whole system can be locked. This offers full protection of the closed system in the event of unauthorized access.

Password syntax can be enforced, giving the option to create greater security by forcing certain characters to be used, e.g. a password must have a capital letter, a number, a special character, and not allowing any of the user-name to be used. This functionality is specific to each user's security demands and so is enabled through VBA giving the full scope of freely definable criteria.

Each user can be logged out automatically after a certain amount of time of inactivity.

'Temporary Login' can be enabled, giving the opportunity when a particular user is accessing a function outside of their authorization, to have a different user enter their credentials, thus then being granted access to the high level function without the need for the first user to logout then login again.

In a zenon networked distributed project where more than one operator from more than one terminal can access the system at the same time, defined functionality can be

enabled to ensure only one person is logged in to a certain system at any given time. A priority system is put in place as to who has access and how the system is released to another operator. This is to protect distributed systems from multiple user conflict, and secures the application to record who is responsible for the events, with their details recorded in the audit-trail. At no time is the system open for unauthorized access.

RGM Recipe Group Management

The recipe group manager in zenon brings all the functionality to handle recipes and their communication to the multiple and different connected systems. The recipe's entire life-cycle management and evolution is embraced in this structure

Each recipe holds values for a certain set of variables, which are communicated to the connected systems when this specific recipe is selected to download. Each recipe has a version number attributed, which is incremented and managed automatically ensuring change management is applied for each recipe. Each recipe can also have a status applied to it, the status are user defined at design time, and allow for a tight quality control over each individual recipe. The recipe status are user configurable to provide flexibility to fit into an existing quality management framework, or to define the ideal quality management system for a given installation.

Recipe name	Recipe version	State	Time of last change	User for last ...	Authorization L...
Filter text	Filter text	Filter text	Filter text	Filter text	Filter text
CIP Low Pressure	1	2 - Released	18.11.2011 08:53:49	SYSTEM	0
CIP	1	3 - Locked	18.11.2011 08:51:17	SYSTEM	0
CIP	2	2 - Released	18.11.2011 09:00:23	SYSTEM	0
CIP	3	1 - Developm...	18.11.2011 08:54:30	SYSTEM	0
CIP High Pressure	1	2 - Released	18.11.2011 08:53:37	SYSTEM	0

Recipe management screen showing the recipe version and recipe state.

User access control is applied in numerous places. Each recipe has an authorization level attributed to restrict modification to authorized persons. When opening a screen the access can be restricted to a specific authorization level, giving the opportunity for only specific recipes to be available for a certain level of operator. For example a production operator or user group may be restricted to recipes which have the status 'Released for production', where all other recipes are not displayed and so cannot be downloaded. A certain operator or user group can be restricted to only allow the latest version of the recipe to be utilized for example.

In the recipe screen there are buttons providing functionality such as 'download recipe', 'save recipe', 'new recipe', 'save as'. Certain functionalities must be restricted, if a production operator is logged in for example only 'released' recipes should be available to be downloaded. Or if a 'released for production' recipe is selected then only the download recipe button is enabled. When a quality manager is logged in then 'Released for production' and 'Recipe in development' recipes may be accessible for downloading. The status may also include 'obsolete recipes' where recipes cannot be saved or downloaded, only copies can be made. This protects each recipe from misuse, within a well defined recipe life-cycle management system.

All RGM activity is logged in the audit-trail. When recipes are downloaded the recipe name only can be listed in the audit-trial, or additionally all the variables concerned with the recipe are also listed, including old and new values. Activity concerning the version

and status of each recipe is logged, also when recipes are created, duplicated, and modified.

Batch Control

The zenon Batch Control module is fully ISA-88 compliant and integrated directly into the zenon system; therefore communication, hardware independence, transparency and protection is integral to the batch design and operation.

User administration is used extensively in the batch module, allowing individual authorization levels to be applied to the different functions contained in Master recipes, Control recipes, and Operations. For example including functions such as: Recipe Start/Pause/Stop, Create recipe, Duplicate recipe, Modify phase, Release Master recipe.

The workflow of a batch recipe development is under a quality management structure. The phases and the links to the physical equipment are defined in the zenon Editor. Certain phase/equipment parameters can be defined at this stage which are critical to the physical operation, and only certain selected parameters are released to be able to be modified at the Master recipe stage. The synchronization between zenon and the physical equipment is defined here, clearly communicating between the two systems when running, pausing, aborting, etc. takes place, thus secure operation is ensured. All variables and functions attributed to the batch control system can be recorded in the audit trail, and be monitored under the alarm management system.

In operation the batch variables can be stored in a zenon archive, linked to the audit-trail and alarm management, and utilize any zenon functionality enabled in the system.

The Master recipe defines the process flow and each parameter values. Certain parameter values can be selected to be changed in the Control recipe.

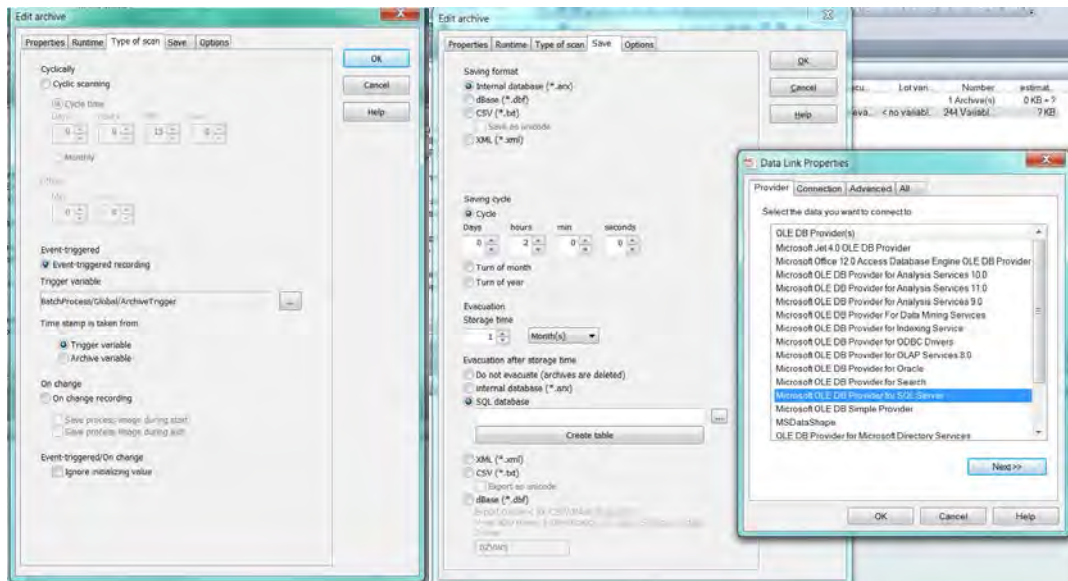
In normal operation, only the Control recipe can execute control. The Control recipe is generated from a Master recipe, and each Control recipe can only be executed once. The Control recipe at any time can be opened and the state of the recipe and the executed values are displayed. Therefore a previously executed recipe can be easily analyzed.

Access to generate new Master recipes, generate new Control Recipes, release Master recipes, execute Control recipes, can be restricted to certain authorization levels, therefore protecting each recipe and its execution from unauthorized operation.

Archiving

The zenon Historian provides the capacity for archiving data. Several storage capabilities are possible: zenon proprietary format, CSV, dBase, and XML. Using the zenon format allows for zenon functionality to access the data inside the archive and present information, such as analysis or reporting. The starting and stopping of archives can be at the runtime start/stop, or via user defined functions from system events, automated events, or user events. Several writing methods can be defined: 'Cyclic scanning' where on a timed basis all defined values are written to the archive, on an 'Event triggered recording' basis where a variable event triggers the write, or 'On change' where when a variable changes its value is recorded. For the 'On change' recording the variable values at the start and end of the archive can be recorded to provide a complete recording of the

variable status for the archive. The archive can also be linked to a batch, thus creating a batch archive recording all events related to a specific batch process.



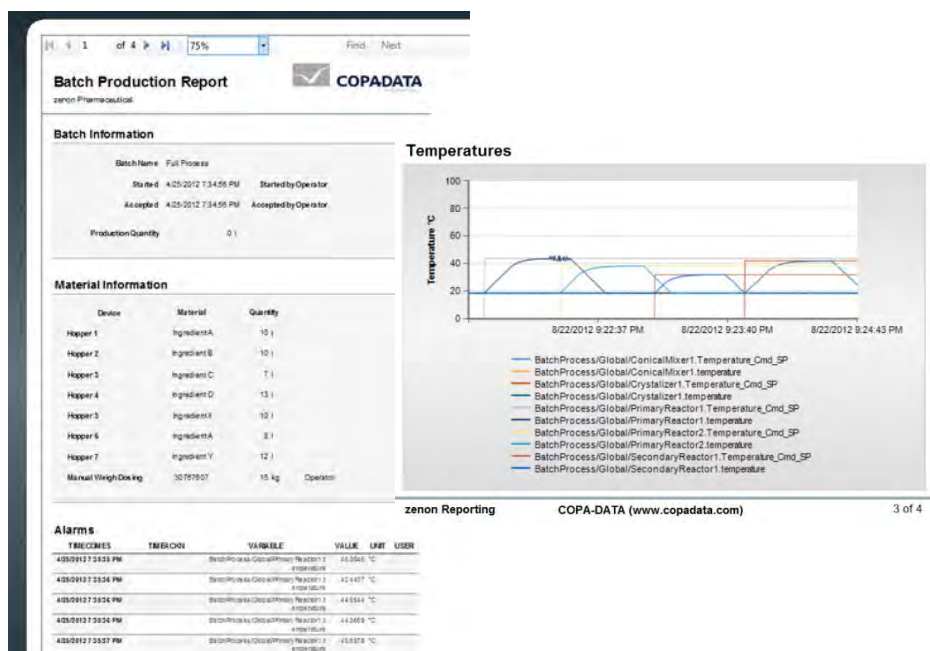
Historian archive configuration with different scanning and export possibilities.

An archive can be selected to evacuate the data to several formats and on a timed basis, this allows for the system to store data for a limited period locally, and then it is evacuated. This evacuation can be locally, or to an external database, in the formats: zenon proprietary format, SQL, XML, CSV, dBase.

Using either the zenon proprietary format or SQL, the archived data can be opened and read back into zenon where analysis can be performed listing variable data, alarm data, and audit-trail information, to be used in the trend analysis module (ETM) or reporting tools.

Report Viewer

zenon has two reporting tools to provide automated documentation possibilities, the Report Generator and the Report Viewer. The Report Viewer uses Microsoft technology to provide advanced reporting capabilities in zenon. The report generator is an historic report tool designed by COPA-DATA, this has several advantages in that it can provide bidirectional read/write to defined variables, this gives numerous operational advantages. The two reporting possibilities are kept for their different functionalities, and to provide backward compatibility.



Report Viewer displaying a sample batch report example.

Full reports can therefore be provided on all system activity, giving the opportunity for example to have production, batch, review by exception (RBE), maintenance, user, and quality reports in each installed application of zenon. Reports can supply data for a given period of time from zenon archives, audit-trail, alarm list, or on-line values. Such functionality opens up the opportunity for standalone GMP functionality.

zenon Logic

zenon Logic is a flexible IEC 61131-3 programming system with an extensive library of functionality directly integrated into zenon, providing SCADA and PLC programming in one system, using only one database. Also SCADA Logic gives greater flexibility to obtain data, process data and control systems or environments at a high level.

This integration merges the HMI/SCADA intelligence and PLC intelligence into one environment. The IEC 61131-3 programming interface zenon Logic is an integral component of the zenon Editor. Both systems access a shared database, utilizing and linking the same variables and data types. As the same database is used for both systems, changes are visible immediately and automatically in both areas, reducing any possibility of error or interfacing risks. Design & process data can be made available in both systems or limited to one system, limiting the scope of usage to the HMI/SCADA environment and/or the PLC environment. zenon Logic offers full redundancy providing security in critical processes. This level of intelligent integration reduces the risk associated with developing multiple systems in tandem, removes the need for designed interfaces between systems, gives a higher degree of functionality through its extensive function library, whilst reducing the validation exposure through the utilization of one database.

Having a 'Used by many library' in zenon Logic provides high levels of functionality whilst reducing the complexity and novelty of bespoke programmed code. Reducing the validation needed and increasing quality in comparison to other programmed environments.

Backward compatibility

The zenon Product Family is continually evolving, backward compatibility is therefore paramount to acknowledge that previous versions of zenon continue to be operational.

Different versions of zenon runtime can communicate and operate together, this means that new systems can be installed along side older systems without the need to update the older systems. From zenon version 6.20 SP4, all system can operate in this manner.

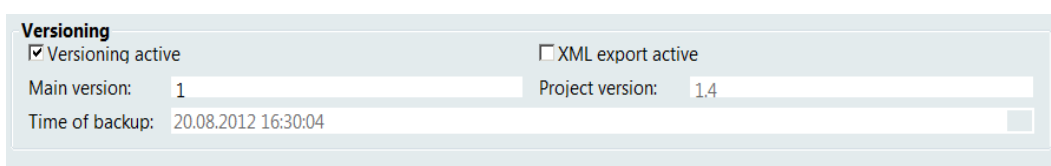
The zenon Editor can open and convert older projects to the current editor version, therefore allowing for previous versions to be continually maintained and modified. The zenon editor can also generate runtime files for earlier runtime installations. This ensures the continued support for any installed zenon application. Design, modification, or evolving previous project to later versions can be applied across all zenon versions, safe guarding all installed systems.

The zenon runtime can also run older versions of zenon projects, this allows for new system to be installed without any change to the validated project.

The full life-cycle of the project, its hardware, and the processes are embrace in this ergonomic culture of compatibility, protecting automation investment.

Project Versioning & Backup capability

Full version control can be administered in zenon projects. In the zenon Editor the designer can request project versioning to be active. The designer selects the major version number, and on each back up of the project the minor version number is incremented. Thus evolution of the project is well defined, and using the 'Restore backup' function any project can be restored to a current or previous version.



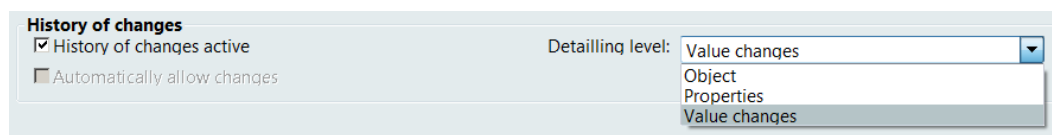
Versioning	
<input checked="" type="checkbox"/> Versioning active	<input type="checkbox"/> XML export active
Main version: 1	Project version: 1.4
Time of backup: 20.08.2012 16:30:04	

Configuration enabling automated project versioning.

Using the 'XML export active' check box all project data is additionally stored in XML format providing two mechanisms to save and restore a project, either as a zenon backup file, or as an XML back file. This opens up the opportunity to allow external versioning tools to gain full access to zenon projects, enabling integration into existing or wider process and equipment change management.

History of changes

In the zenon Editor any design or configuration change can be logged, therefore giving a clear record of all changes with the name of the designer, the time stamp, and the item which has changed with 'from' and to 'values'. Validated project can therefore be monitored, and the qualification process can utilize this information to specifically target the changes made.



Enable 'History of Changes' with selectable detail level.

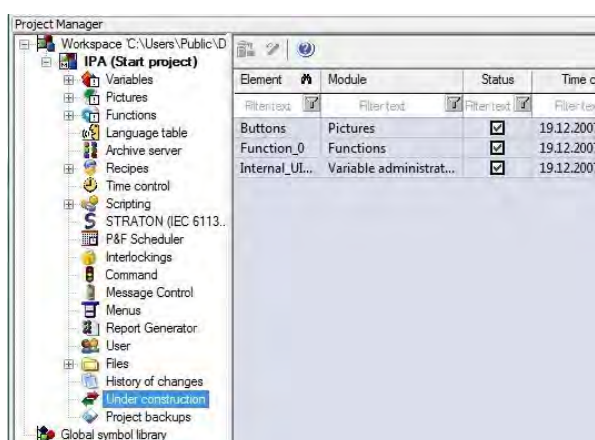
Displaying the changes made to a validated project, gives a clear report on where qualification of the project is needed to re-validate the changed operation of the project.

Different levels of detail can be recorded, selecting either 'Object', 'Properties', or 'Value' determines the level of detail the history records. With 'Values' selected all modification data is recorded, e.g. if a certain button is moved the object is the button, the properties are 'X' & 'Y', with values changes giving the actual 'From' and 'To' values.

Distributed Engineering

zenon has the possibility to have Distributed Engineering projects, where a project can be simultaneously worked on from different workstations at the same time. In this case a specific user is allowed access to a certain area of the project, and their work can then be accepted into the project or rejected. This allows for changes to be checked before being applied to the project.

In this mode of operation, before editing of a particular section of the project is carried out, this specific section needs to be checked out. After the changes have been made, the authorized user then synchronizes the project, and accepts or rejects the changes. This method can be used in all projects to restrict and control project evolution in accordance with a Quality Management System.



The checked out elements of the project are listed in the 'Under Construction' project manager node, displaying the name of the user, status, and the element name.

5. zenon Pharma Edition

zenon Pharma Edition provides enhanced functionality which embraces the unique environment of pharmaceutical projects and their life-cycle from concept to retirement. Aiming to ensure the highest productivity of automated equipment whilst impacting on the validation effort and cost associated with projects in regulated environments.

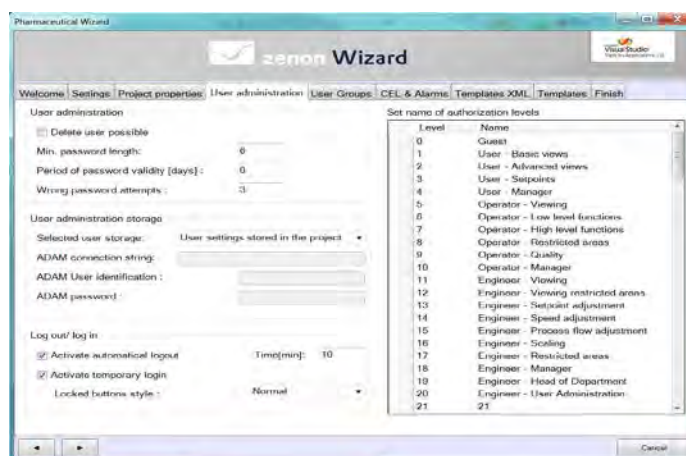
Regulated GMP projects have distinct project behaviour and demands, where qualification and validation is enforced in order for the secure operation of processes controlled within them. Each regulated company has a unique structure and workflow to achieve their model of Part 11 compliance. In this regard one aim of the zenon Pharma Edition is to provide functionality and tools which address the ideals of validation and change management of a project, and carry forward the philosophy of design once and reuse.

The zenon Pharma Edition contains several tools such as: Pharma wizard, Comparison wizard, Documentation wizard; which provide a framework of regulation for zenon projects, which aims to allow a certain regulated company model to be efficiently applied.

Pharma Wizard

This zenon Editor tool offers functionality to provide a framework for regulation, making design and validation of projects much easier and more efficient.

The pharma wizard provides a central location for all project generic regulatory parameters, locating one place to design and modify project behaviour for GMP projects. This single location also makes qualification easier to verify that certain mechanisms are in place.



The zenon Pharma wizard standardizing regulated project behaviour.

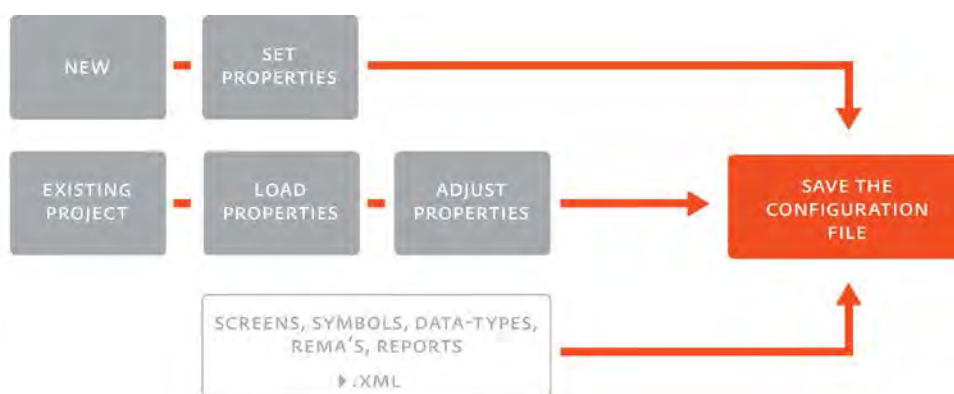
The second part of the pharma wizard is to include templates for Screens, Symbols, Variable data-types, Reaction matrix, Reports, and Colour pallets, of which default templates are provided and of which more can be added by the user. The templates together with the project behaviour parameters provide the required generic GMP functionality for regulated projects. The profile is stored as a configuration file. This file can then be used again & again to provide the same functionality to other projects, or create new projects with this functionality and project behaviour. Therefore providing all

the generic regulation aspect of a project, its behaviour, and the elements to use the behaviour at a click of a button.

All GMP projects have the same basic needs and principles involving: audit-trail, alarms, archives, reports, user administration; this project behaviour and functional templates to use it are contained and managed in the pharma wizard.

Holding such behaviour and functionality in a configuration file offers many advantages, reduced risk due to less human intensive operations, standardize on a specific security profile of projects, and to have a generic quality documentation that is matched to the configuration file. Having the goal to reduce the validation effort, with a design once, test, qualify, and then reuse many times.

This extends COPA-DATA's philosophy of efficient engineering, to the largely manual and intensive validation exercise each project is required to undergo.



Creating the configuration file.



New projects can be created with all the required GMP project behaviour and functionality through the Pharma wizard.



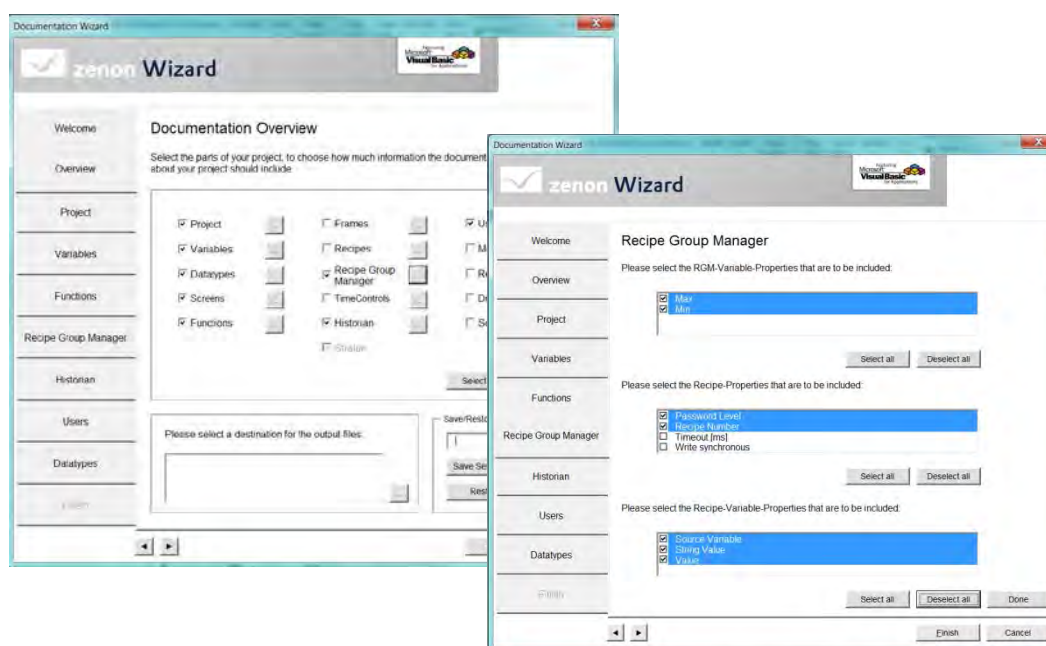
Existing projects can be aligned with the configuration profile, ensuring the defined project security is enforced and compliance is achieved.

Documentation wizard

The zenon Editor has a documentation wizard, in which the user can automatically obtain a paper document detailing the project content and behaviour. This covers the full scope of the project, in which the user can select certain areas and the level of detail needed.

Such a document can hold the project behaviour details for GMP specific elements such as: Audit-Trail, Alarms, Users, Users groups, User Authorizations, Archives, Reports, Screens and their content.

The documentation wizard provides a hardcopy summary in a human readable format.

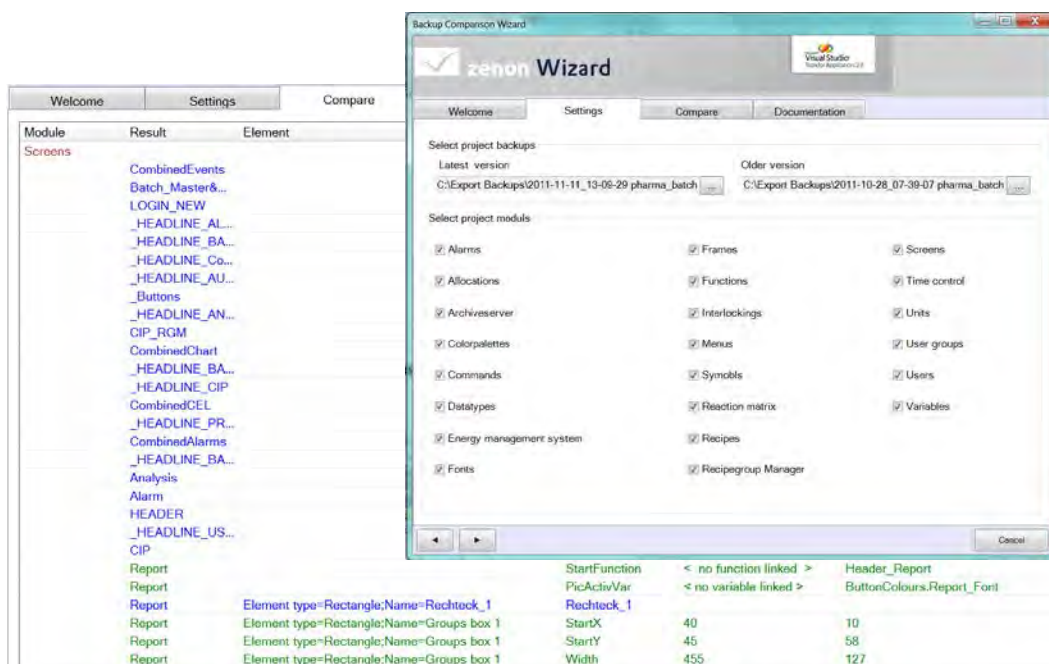


Selecting the included content and level of detail for a project document.

Comparison wizard

Within the scope of project versioning in the zenon Editor, two backup projects can be selected and compared, the resulting analysis displays the differences between the two projects including: Added elements, Deleted elements, and New elements. A printable version is also generated providing a hardcopy of the comparison.

If the two projects being compared are two versions of the same project, the evolution of the project is clearly identified, therefore aiding the testing and qualification needed by the change. If the projects are a comparison between a benchmark and a design project, the project is therefore tested against a know good GMP profile, and any differences in the regulation aspects are clearly identified.



Selecting the elements to include in the example comparison report.

In combination

The combination of the Pharma wizard, Documentation wizard and Comparison wizard, provides a proven project behaviour and functionality for GMP environments. Giving documented evidence of how the project behaves. And providing comparison between projects displaying the risk associated with any change, and clearly displays the areas which are impacted by the change requiring further qualification and validation.

Effectively managing regulated projects and their life-cycle, to positively impact on the validation effort needed, and reduce the associated risk of regulated projects.

6. COPA-DATA quality management

COPA-DATA has quality management systems in place as internal procedures, which ensure our zenon Product Family is designed, developed, and maintained in accordance with strict quality criteria for consistent high quality and reliability.

Product development management

The HP Quality Center provides the backbone to our software development quality management. Covering each product element in detail from specification or defect, through design, development, testing and release into the zenon Product Family products.

All product research and development is conducted within COPA-DATA. Our development professionals employ two methods for software project engineering and planning: V-Model Software Development, and Scrum Agile Software Development. Both project development streams utilize HP Quality Center and Microsoft Project providing secure planning and management of the development and release procedures. All change and version control is recorded and documented in detail.

Our implementation of the HP Quality Center integrates strong internal procedures and workflows. This allows for full traceability and visibility giving details of each revision step with user requirements, defects, user specifications, design specifications, development information, testing criteria, with test results detailing verification and how acceptance is achieved and documented before release. All products developed by COPA-DATA are under full traceability throughout their life-cycle.

Authenticity at this level is ensured through user administration safe guarding content on viewing, modification, creating, and deletion; for data, procedures, or documentation. Digital signatures are required for testing, qualification, and release of product elements.

Automated processes defined in the HP Quality Center ensure each product and development stage is carried out under the strict procedures we have set, thus consistency and reliability is established.

Human Resource Management

Employee education, assessment, and training is undertaken as a culture of excellence. On a continual basis COPA-DATA holds several internal academy trainings and communications for employees covering different areas of company and product development. Trainings are also offered via our online training system for international partners.

External audits

COPA-DATA is fully open to be audited by regulated customers. COPA-DATA has a long history in several regulated environments, auditing in many forms and detail has previously been successfully accommodated.

7. Part 11 compliance table

Subpart B—Electronic Records

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
11.10	<p>Controls for Closed systems</p> <p>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.</p>	<p>Customers are required to have applications, process, and operating procedures that ensure a closed system is in place and maintained, with periodic auditing being performed ensuring the continued integrity of the system(s).</p>
11.10 (a)	<p>Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p>Validation of the system must be undertaken within a culture of life cycle management to ensure the machine and processes are fit for the intended purpose.</p> <p>The ISPE GAMP guidelines provide recommendations on validation principles, including testing or verification requirements and documentation which will qualify the system that it performs its intended purpose defined by the design.</p> <p>zenon provides several tools to assist in the validation process. zenon Pharma edition has several tools to apply a known project behaviour profile, a documentation tools to provide a hardcopy of the project contents and behaviour, a comparison wizard to identify differences in projects highlighting the changes and risk needing verification.</p>
11.10 (b)	<p>The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any</p>	<p>Data in zenon is saved in its own proprietary file formats or in a SQL database.</p> <p>The individual data can be accessed in many ways:</p> <p>i) zenon has reporting capabilities,</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
	<p>questions regarding the ability of the agency to perform such review and copying of the electronic records.</p>	<p>proving combined or individual documents for Audit-Trail, Alarm lists, Archives, and online values.</p> <p>The data is provided as a screen report, hardcopy, or electronic 'pdf' format. Allowing reading and archiving of the data.</p> <p>ii) Integrated tools of zenon includes Audit-Trail, Alarm management, and Archive revision screens for reading, listing and commenting.</p> <p>Data can be stored in the proprietary formats, and accessed via the zenon tools at a later time.</p> <p>iii) Data can be exported into different formats (dBase, Ascii/CSV, XML, SQL) and then displayed and archived in external systems.</p> <p>iv) Data can directly be stored in a relational SQL database. External programs can access data there via authorized access.</p>
11.10 (c)	<p>Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p>Data are stored in zenon specific binary files, which can be secured by the security system of the Windows file system.</p> <p>The location of the data can be specified by the user, and so can be placed on a secure server with its own protection and security measures.</p> <p>Customers should establish policies and procedures to ensure that records are retained for an appropriate duration of time.</p>
11.10 (d)	<p>Limiting system access to authorized individuals.</p>	<p>zenon's User Administration and authorization is integral to all functionality contained, zenon has local internal User Administration, and Active Directory capabilities connecting IT systems, both systems can be used concurrently. Biometric and external security identification devices are accommodated. Utilizing zenon's authorization levels different layers of security can be applied to different users or user groups.</p> <p>Access to the closed system is therefore provided. Each dynamic element that a user has access to can</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
		<p>have an authorization level attributed, before the function of this dynamic element is executed the logged on user must hold the specific authorization level.</p> <p>Password aging, password length is enabled in zenon. False login attempts are protected against with detection of password error and user ID error, locking out the user and system respectively when a certain number of erroneous login attempts have been made. Each successful and unsuccessful login attempt is recorded in the audit-trail.</p> <p>Each zenon project should utilize the automatic user logout function which logs out a user after a defined period of time.</p> <p>Procedures can therefore be in place to define who is authorized access to the system, and where they are allowed access.</p> <p>When accessing a system remotely, functionality is included to allow only one person access to the system at any given time, and protocols are in place to request access and logout other users.</p> <p>Procedures should be in place at the operating system level to restrict user access across the PC system.</p>
11.10 (e)	<p>Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.</p>	<p>All user, automated events, and systems events can be included in the audit-trail. The audit-trail includes multiple information concerned with each event including: time-stamp showing date & time of the event, variable name, variable identification, full user name, computer or system name, project/application name, variable value (with old & new values on user change), variable status, alarm text, alarm area & alarm class. With the possibility for a user to add a comment on all events.</p> <p>zenon has a built in clock synchronization to ensure that all date and time stamps are accurately recorded in the audit trail. It is also possible on certain PLC drivers to have</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
		the PLC time used as the time stamp.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The sequencing of user step, automatic steps and operational checks can be developed using the integral zenon functionality, to force a user to follow certain procedures at certain phases of the systems execution.
11.10 (g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	<p>zenon's User Administration and authorization is integral to all functionality contained, zenon has local internal User Administration, and Active Directory capabilities connecting IT systems, both systems can be used concurrently. Biometric and external security identification devices are accommodated. Utilizing zenon's authorization levels different layers of security can be applied to different users or user groups.</p> <p>Access to the closed system is therefore provided. Each dynamic element that a user has access to can have an authorization level attributed, before the function of this dynamic element is executed the logged on user must hold the specific authorization level.</p> <p>Password aging, minimum password length and syntax complexity is enabled in zenon. False login attempts are protected against with detection of password error and user ID error, locking out the user and system respectively when a certain number of erroneous login attempts have been made. Each successful and unsuccessful login attempt is recorded in the audit-trail. Each zenon project should utilize the automatic user logout function which logs out a user after a defined period of time.</p> <p>Procedures can therefore be in place to define who is authorized access to the system, and where they are allowed access.</p> <p>When accessing a system remotely, functionality is included to allow only one person access to the system at</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
		<p>any given time, and protocols in place to request access and logout other users.</p> <p>When performing a protected operation there are several levels of protection, the currently logged in user can be applied, the user can be requested to login for this specific request, and the user can be requested to give a reason for the action. All of which is recorded in the audit-trail.</p>
11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	<p>Data input can be restricted to defined stations, therefore limiting actions to specific locations. zenon client/server architecture restricts data storage to the server computer only, ensuring that the audit trail is generated from a single location.</p> <p>The audit trail records each variable driver and user location, therefore the origin of the event is always clearly indicated.</p> <p>All zenon drivers include status information about the quality of the connection and the quality of each individual value, which is recorded in the audit-trail. This same mechanism is in place in the zenon network Client/Server and Redundancy communication.</p>
11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	<p>It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task.</p> <p>Utilizing Active Directory possibilities within zenon User Administration means that each zenon project is automatically included in the wider User Management structure within an organization. Such a user management system would provide the processes to included the required education and training proof before access is granted.</p>
11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature	It is the responsibility of the customer to ensure that all individuals who develop, maintain, or use the systems are properly educated to perform their task.

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
	falsification.	All user events are recorded in the audit-trail, requiring authorization to the system before any actions can be initiated ensures the event is linked to the user and the signature is linked to the record. The audit-trail is a binary file where individual modifications external to zenon are not possible.
11.10 (k)	Use of appropriate controls over systems documentation including:	
11.10 (k-1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	<p>Access can be protected within zenon as to who has access to certain documentation, and who can instruct the exportation of data.</p> <p>All data is stored in proprietary system binary files, which cannot be modified externally to the zenon system.</p>
11.10 (k-2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	<p>zenon has several measures in place to accurately control, document, and backup project evolution and modifications.</p> <p>Version control can be implemented in the zenon editor where utilizing Major and Minor project revision numbers strict control of the project evolution can be enforced. The Major revision number is user defined, the Minor revision number is incremented automatically after each project backup.</p> <p>Using the XML backup option, external systems can be used to provide version and change control, with full backup capability in zenon.</p> <p>With the project backup mechanism previous projects can be restored, giving protected from the associated risk of modification.</p> <p>zenon editor has a 'History of Changes' mechanism, where any changes to a project is recorded in detail. All changes and modifications can be easily identified.</p> <p>zenon has a project comparison tool which provides a detailed account of the difference between two projects, displaying Modified, Additional, and Deleted project elements. When used in combination with the project versioning, a clear document is provide</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
		of the evolution the project has undergone, in order to highlight the risk and validation testing that must be performed.
11.50	Signature manifestations	
11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	
11.50 (a-1)	The printed name of the signer;	The audit-trail and alarm list (CEL and AML) records each event including the time-stamp showing date & time of the event, variable name, variable identification, full user name, user ID, computer or system name, project/application name, variable value with old & new values on user change, variable status, alarm text, alarm area & alarm class. With the possibility for a user to add a comment on all events. Include date and time stamp, node of origination, and operator name.
11.50 (a-2)	The date and time when the signature was executed;	
11.50 (a-3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	
11.50 (b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	<p>Data in zenon is saved in its own proprietary file formats or in a SQL database.</p> <p>The individual data can be accessed in many ways:</p> <p>i) zenon has reporting capabilities, proving combined or individual documents for Audit-Trail, Alarm lists, Archives, and Online values.</p> <p>The data is provided as a screen report, hardcopy, or electronic 'pdf' format. Allowing reading and archiving of the data.</p> <p>ii) Integrated tools of zenon includes Audit-Trail, Alarm management, and Archive revision screens for reading, listing and commenting.</p> <p>Data can be stored in the proprietary formats, and accessed via the zenon tools at a later time.</p> <p>iii) Data can be exported into different formats (dBase, Ascii/CSV, XML, SQL) and then displayed and archived in external systems.</p> <p>iv) Data can directly be stored in a relational SQL database. External</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
		<p>programs can access data there via authorized access.</p>
11.70	<p>Signature/record linking.</p> <p>Electronic signatures and hand-written signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.</p>	<p>Each audit trail record includes the name of the operator linked to the specific activity.</p> <p>All user events are recorded in the audit-trail, requiring authorization to the system before any actions can be initiated ensures the event is linked to the user and the signature is linked to the record.</p> <p>When performing a protected operation there are several levels of protection, the currently logged in user can be applied, the user can be requested to login for this specific request, and the user can be requested to give a reason for the action. All of which is recorded in the audit-trail.</p> <p>The audit-trail is proprietary binary format therefore individual modifications are not possible external to the zenon system.</p> <p>Customers should also establish policies and procedures to prevent unauthorized access to audit trail files (AML, CEL), which can be done with the security system of the Windows file system.</p>

Subpart C—Electronic Signatures

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
11.100	General requirements	
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	zenon local user administration and Windows Active Directory do not permit the creation of duplicate login's or user ID's. The user is required to enter an ID and a password to gain access to the system, ensuring each user is unique, clearly identifies the individual user, and who's credentials cannot be used by another person.
11.100 (b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	<p>Customers using zenon applications in FDA-regulated environments are responsible for ensuring that electronic signatures are unique to one individual and not reused by or reassigned to any other individual.</p> <p>Customers using zenon applications in FDA-regulated environments are responsible for verifying the identities of individuals using electronic signatures.</p>
11.100 (c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	Customers using zenon applications in FDA-regulated environments are responsible for verifying the identities of individuals using electronic signatures, and that each user fully understands the implications of applying an electronic signature.
11.100 (c-1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	<p>Correct procedures must be in place to physically identify each user of the system.</p> <p>Utilizing Active Directory possibilities within zenon User Administration means that each zenon project is automatically included in the wider User Management structure within an organization.</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
11.100 (c-2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Customers using zenon applications in FDA-regulated environments are responsible for verifying the identities of individuals using electronic signatures, and that each user fully understands the implications of applying an electronic signature.
11.200	Electronic signature components and controls.	
11.200 (a)	Electronic signatures that are not based upon biometrics shall:	
11.200 (a-1)	Employ at least two distinct identification components such as an identification code and password.	<p>The zenon user administration and Windows Active Directory user administration demand the input of a 'User-ID' and a 'Password'.</p> <p>External security identification systems can also be accommodated in zenon, the responsibility to provide adequate identification of specific users with the required two distinct components then falls to this external security system.</p>
11.200 (a-1-i)	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	<p>To indicate the start of a continuous period of controlled system access, the user must use 'User-ID' and 'Password' to log into zenon.</p> <p>For subsequent signatures during this period zenon security requires the user to enter all signature components.</p> <p>The zenon 'User Login Timeout' period should be configured to limit the extent of a continuous period of controlled system access. Customers should also implement policies and procedures requiring users to log out of the application during periods of non-use.</p>
11.200 (a-1-ii)	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	<p>The zenon User Login Timeout period should be configured to limit the extent of a continuous period of controlled system access. Customers should also implement policies and procedures requiring users to log out of the application during periods of non-use.</p> <p>The user has to enter all signature components for all signings by default.</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
11.200 (a-2)	Be used only by their genuine owners;	<p>Customers using zenon applications in FDA-regulated environments must be responsible for ensuring that non-biometric electronic signatures are used only by their genuine owners.</p> <p>Each User-ID must be linked to an individual person, sharing of ID's is not possible, and group ID's are not allowed.</p>
11.200 (a-3)	Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	<p>Customers using the zenon applications in FDA-regulated environments are responsible for ensuring that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. For example, When using Windows Active Directory organizations must require that system administrators enable the Windows security function "User Must Change Password at Next Logon" in order to prevent the system administrators from knowing both the user's user ID and password.</p> <p>Within the local zenon user administration when the administrator has reset the password, zenon security automatically demands a new password the next time the user logs in.</p>
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. issuance amendment, or revocation of an order.	<p>Biometric security identification systems are accommodated in zenon. The responsibility that electronic signatures based upon biometrics are designed to ensure that they cannot be used by anyone other than their genuine owner falls to this external security system.</p>

Regulation Section	FDA 21 CFR Part 11 Regulation Text	zenon statement
11.300	<p>Controls for identification codes/passwords.</p> <p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</p>	
11.300 (a)	<p>Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.</p>	<p>zenon local user administration and Windows Active Directory do not permit the creation of duplicate login's or user ID's. The user is required to enter an ID and a password to gain access to the system, ensuring each user is unique, clearly identifies the individual user, and who's credentials cannot be used by another person.</p>
11.300 (b)	<p>Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).</p>	<p>The zenon local user administration and the Windows Active Directory security shall be configured to use the functionality for password aging.</p>
11.300 (c)	<p>Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.</p>	<p>The user administrator for zenon local user administration or Windows Active Directory has the authority to enable and deactivate user accounts.</p> <p>When using external security systems to provide logging in credentials to the zenon system, the responsibility falls to the administration of these external systems to provide adequate loss management.</p>
11.300 (d)	<p>Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</p>	<p>False login attempts are protected against with detection of password error and user ID error, locking out the user and system respectively when a certain number of erroneous login attempts have been made. Each successful and unsuccessful login attempt is recorded in the audit-trail.</p>
11.300 (e)	<p>Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.</p>	<p>When using such external security systems to provide login credentials to the zenon system, the responsibility falls to the administration of these external systems to provide evidence of correct function and that periodic testing has been carried out.</p>



© 2012 Ing. Punzenberger COPA-DATA GmbH

All rights reserved.

Distribution and/or reproduction of this document or parts thereof in any form are permitted solely with the written permission of the COPA-DATA company. The technical data contained herein have been provided solely for informational purposes and are not legally binding. Subject to change, technical or otherwise.

www.copadata.com/pharmaceutical