BellHawk®

Real-Time Materials Tracking and Traceability Software

www.BellHawk.com

BellHawk Data Sheet
Part 11 Compliance

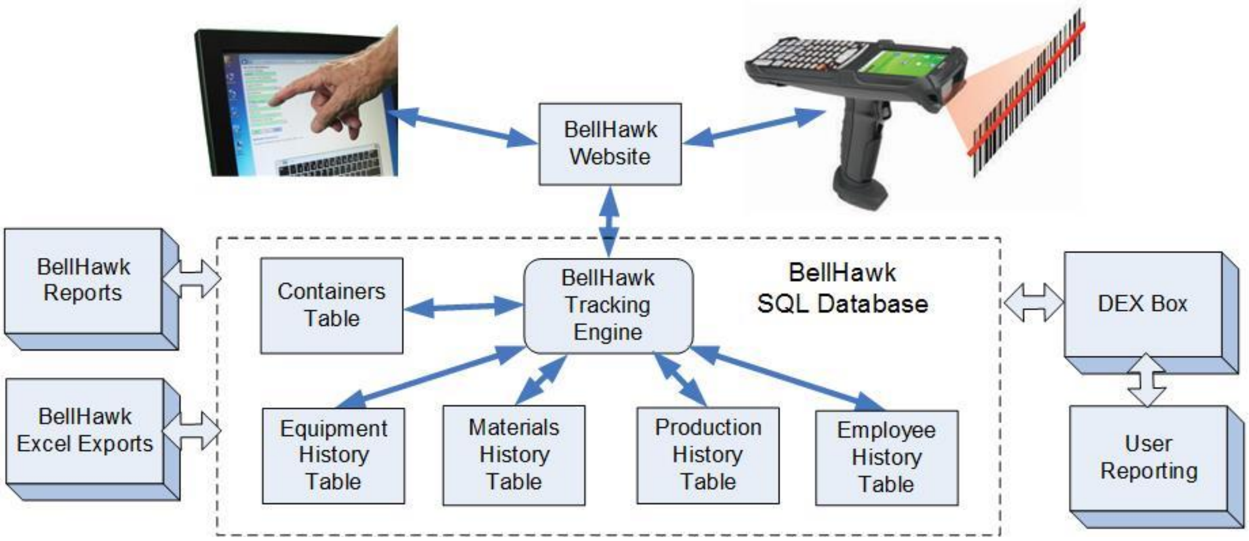
Introduction

This document details the compliance of the BellHawk® software with “CFR 21 Part 11” (Part 11) dated March 20, 1997 and the guidance document “General Principles of Software Validation; Final Guidance for Industry and FDA Staff,” issued January 11, 2002 by the FDA.

The intellectual property rights for BellHawk are owned by Milramco LLC. The BellHawk software was developed by and is maintained by partners of Milramco.

Capture of Electronics Traceability History

The BellHawk software records the receipt and put-away of raw materials, their transformation into intermediate and finished products, as well as tracking work-in-process. In addition, BellHawk tracks the picking, packing, labeling, and shipping of finished products to customers and distribution centers.



As well as maintaining the current status of all containers of materials that it tracks, BellHawk also tracks the history of all transactions performed on materials, including the transformation of materials in production, as well as the people involved and the equipment used.

This data can then be interrogated through a series of standard reports and Excel exports, as well as used for materials traceability (one step forward, one step back) purposes using the BellHawk TRACE module. Capabilities exist for custom reporting on this data, such as through the DEX interface.

This data is retained perpetually in the BellHawk database. If this data is modified by a supervisor or manager to correct mistakes, such as wrong quantity or lot number, then a complete audit trail of such changes is maintained with the supervisor’s name and reason for making the changes.

Electronic Signatures

BellHawk supports the use of an encrypted data link between the device on which the web-browser, used to access BellHawk, is running and the Windows Server computer on which the BellHawk code is executed and through which the SQL Server database, used to record the electronic record data, is accessed.

Each data collection device and external system that accesses the BellHawk software has its own encrypted login, thereby securing device access. Each employee using such a device is required to identify themselves by a means of scanning a barcode whenever they record transactional data, to identify who is recording the data. Optionally each employee can be required to have their own personal login, in addition to scanning their badge into a data entry device, thus meeting the requirement for two separate forms of identification, where needed.

Optionally BellHawk can print out documents, such as batch processing records, with places for physical signatures by employees recording materials into and out of a batch processing operation, as an extra visual layer of compliance.

All transactional data recorded in the BellHawk database is time tagged to the nearest second and identified as to who the person making the entry was.

BellHawk requires the use of a user name and password for all staff members accessing the BellHawk system. Staff members have review and electronic sign-off requirements on all data entered into the system, as appropriate to their management and supervisory role. All changes to the database records made by a staff member are recorded, with the retention of the original record and a recording of who made the changes.

All passwords are stored in the BellHawk database in non-reversible encrypted format. They can only be changed by the system’s administrator, who is a trusted employee, with his or her own encrypted password. It is the responsibility of the system’s administrator to ensure that appropriate password aging and control procedures are followed.

Permanence of Data Records

Data within the BellHawk database cannot be deleted through the BellHawk user interface or external interfaces. Data can only be modified by direct access to database by the client's Information Technology (IT) staff who have such trusted privileges. It is incumbent on our clients to ensure that their IT practices related to the protection of the data in the database follow good IT practices for security and limitations on data access.

Any data record "deleted" by a user through the BellHawk user interface or the web-services interface are not physically deleted but are simply marked as deleted so as to be not visible to the user. These records can be recalled at any time for audit purposes.

All changes made to data records are logged as to who made the change and the time and date that the change is made. These data records are kept in permanent history tables as well as logged to a daily audit trail log as described in the next section.

It is critical that the client's IT staff take a full backup of the database and daily audit log files at least daily and store this backup data in an off-site location from which it can be quickly retrieved in the event of need for disaster recovery.

Audit Trail

BellHawk can produce a daily log file of all new entries and updates made to the BellHawk database. This log file is in standard extended ASCII human readable format. Log files can be downloaded through the manager's switchboard.

The data recorded in each record in the file includes:

1. The time and date in UTC (universal time code) format
2. The person making the entry with first name, last name and employee number
3. The keyword for the data object, such as ITEM for a change to an item master record
4. The new parameters in JSON (JavaScript Standard Object Notation) standard format, such as {"ItemNumber": "ABC123", etc }

A new log file is produced each day, with a file name that includes the date of the day on which the file was produced.

If errors occur during the operation of the system, they are included in the same log file.

Software Development Practices used for BellHawk

BellHawk was developed and is maintained according to good software development practices, as described below.

Version Control

Milramco maintains a complete on-line database of all past versions of the BellHawk software, from using the Subversion software. This includes the standard version of BellHawk as well as special modifications made for each client. Subversion enables the BellHawk development team to track all changes made and to recover prior or alternate versions upon demand.

Each release of BellHawk is clearly shown with its version and subversion number on each user screen to aid in tracking down any issues that may arise.

Upgrades

1. All proposed changes to the software are documented in writing by a qualified system's architect (M.Sc. or Ph.D. in Computer Science plus at least 10 years' experience). This document is then reviewed and approved by the originator of the request and the software development team and any needed changes made before a final specification document is issued.
2. The needed changes are then broken down into a series of tasks that can be accomplished by a single software developer. Each task is assigned to a senior software developer (with typically a Master's degree education in Computer Science and 10 years plus development experience) who may make the changes themselves or supervise more junior people in making the changes.
3. The tasks are logged as "tickets" in an on-line status tracking system, so their status can be tracked.
4. The resultant code changes for each task are then functionally tested by the assigned senior software developer to ensure compliance with algorithmic and database access requirements.
5. The resultant code changes are then reviewed or tested to requirements set by a systems architect to ensure compliance with the written specifications.
6. The resultant code changes are then tested by the requestor.
7. If any discrepancies are found, they are logged in Milramco's on-line ticket tracking system and assigned to appropriate people to be fixed, then retesting takes place, as appropriate.

Bugs and Errors

1. Bugs or other errors are logged in Milramco's on-line ticketing system along with their priority.
2. Problems are typically investigated by a senior software developer, who will test the software or evaluate the contents of a backup database, taken as soon as possible after the incident, to determine the cause of the problem.
3. If the cause is a data entry error on behalf of the client using the software then they will be so notified and charged for the time taken to investigate the problem.
4. If the cause is system design problem then the issue will be investigated by a system's architect may issue an upgrade request and the above upgrade process will be followed.
5. If the cause is a bug in the code, then a fix will be coded and tested by the programmer and tested by a senior programmer.

6. The bug fix will then be tested by the client or system's architect reporting the bug.
7. The status of the problem report is tracked through our on-line ticket tracking system until it is satisfactorily resolved.

Level of Compliance

The BellHawk software is a decision support system which is designed to assist trained and knowledgeable personnel in collecting and maintaining one-step forward, one-step backward traceability records and rapidly recalling that data when needed. It is not intended for use as a fully automated data collection system nor is it suitable for use in any application where any action of the software could directly cause harm to, or negatively impact the safety of, any person or animal.

BellHawk is purely a data collection and reporting system. Its results should only be used by trained and knowledgeable personnel to assist them in their decision-making processes. Such personnel must use their training and judgment in the interpretation of all reports and Excel exports produced by the BellHawk software.

BellHawk follows the implementation guidance documents published by the FDA to the extent that they are appropriate to a low-risk deployment in capturing materials tracking and traceability data for subsequent analysis by skilled personnel who are appropriately trained.