Audit Trail Requirements for Software Update

Tom Fink

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Change** |
| July 5, 2012 | 1.0 | Tfink | First Revision |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Background

* At the March 2012 NCWM Software Sector Meeting, it became apparent that the NTEP Adminstrator (Jim Truex) interprets Handbook 44 (HB44) to require updates of metrologically significant software to be recorded in the Audit Trail. See the “Software Update Audit Trail Issue” document for details of what was said at this meeting and why we think it’s in our best interest to comply with Mr. Truex’s interpretation of HB44.
* As time allows, our existing products will be updated to increment the Audit Trail as required by Mr. Truex’s interpretation of HB44. In addition, all references to Remote Firmware Updates will be removed from the sales literature and the scale Supervisor & Service manuals.
* The purpose of this document is to specify the requirements needed to meet HB44 requirements for software updates.

# Definitions

* Category 1 Audit Trail
  + Consists of two Event Counters: A “calibration parameters counter” and a “configuration parameters counter”.
    - The value of these counters must be displayed on the scales “Weights and Measures” screen.
  + All Hobart scales currently implement a Category 1 Audit Trail.
* Category 3 Audit Trail
  + A category 3 Audit Trail is an event logger. The following must be recorded for each “event”: the event number (000 to 999), the parameter ID, the date and time of the change, and the new value of the parameter. A printed copy of the information must be available through the device or through another on-site device. The event logger must have the capacity to retain records equal to ten times the number of sealable parameters in the device.
* HB44: Handbook 44 – The document containing US Weights and Measures Requirements

# Requirements Overview

* HB44 SW Update Audit Trail requirements are different for scales that have remote update capability and scales that can only be updated at the scale.
  + Scales with no remote update capability are only required to have a Category 1 Audit Trail. In this case the Configuration Event Counter must be incremented whenever there is a metrologically significant software change.
  + Scales with remote update capability are required to have a Category 3 Audit Trail. In this case the Software Version parameter must be updated to show the date and time of the change and the version of the new software.
* It is still up to the manufacturer to determine if the software changes are metrologically significant. The Audit Trail only has to be updated for metrologically significant software changes.
  + If there is no way to distinguish metrologically significant software updates and non-metrologically significant software updates, all updates must be considered metrologically significant.
  + There is not yet a requirement for a portion of the version number to indicate a metrologically significant change, but having one would make it easier to explain to Field Inspectors why the software version has changed but the Audit Trail hasn’t been updated. In addition, this would be a good way for the “updater code” to determine if the new code contains metrologically significant changes.

# Requirements for “At the Scale” Update

* Whenever a metrologically significant code change is made the “Configuration Counter” of the Audit Trail must be incremented. That’s it.
  + This change should be relatively easy to implement on existing hardware for all production scales.

# Requirements for Remote Update

## Overview

* Any scale that has remote software update capability must implement an “Event Logger” to meet the Category 3 Audit Trail requirement. The software update must be logged as an “event” in the Event Logger.

## Event Logger Requirements

* The Event Logger must contain the following fields:

|  |  |
| --- | --- |
| **Field** | **Field Description** |
| Event Counter | 000-999 (roll over after 999) |
| Parameter ID | A description of the Parameter |
| Parameter Change Date | Must included the month, date, and year (DES-134) |
| Parameter Change Time | Must include Hour and Minute. I’m assuming it must distinguish between AM and PM or use military time. |
| New Parameter Value | Value will vary from parameter to parameter (see table below). |

* Other Event Log Requirements
  + The number of recordable events must be greater than or equal to the number of 10 times the number of sealable parameters, but does NOT have to be greater than 1000 records.
  + A method of printing the event log must be provided via the device itself (i.e. the label printer) or through another on-site device (i.e. a network printer). The printout must exclude nonmetrological information (DES-134).
  + When a device is being remotely configured or updated it must be disabled or indicate that it is in “configuration mode” (DES-135).
* Event Log Options
  + Additional relevant information is permitted, such as the old value of the parameter that was changed (DES-134).
* HLX Parameters
  + The following table lists the parameters in the HLX that must be included in the event log.
    - Other scales may have other parameters.
    - There’s a lot of parameters in the Serial EEP that are no longer used. It would make sense to eliminate them on future weighers.

|  |  |  |
| --- | --- | --- |
| **Parameter Description (ID)** | **Data Type1** | **Comment** |
| Peripheral Controller Software Major Version | UINT |  |
| Peripheral Controller Software Minor Version | UINT |  |
| System Controller Software Version | ? | Should probably update version format to X.Y.Z where ‘Y’ = the Metrologically Significant Version Number |
| Center of Maintenance Zone | LINT (4 Bytes) | Changes when scale is calibrated. Not directly entered by user. |
| Scale Factor | LINT | Entered in Wgr Service Screen (Division Size field). Configures scale for Single Range or Dual Range. |
| Max Weight | LINT | Entered in Wgr Service Screen |
| Gain\_Factor | LINT | The scale gain factor. Changes when scale is calibrated. Not directly entered by user. |
| Zero Reference | LINT | Used to determine if the Power Up zero is within the allowable range. Updated by software during calibration. |
| ~~Calibration Reference~~ | LINT | Not used on peripheral controller. Not used on System Controller either? |
| ~~Rate Option Time~~ | UWORD | Not used on peripheral controller. Not used on System Controller either? |
| ~~Auto Zero Maintenance Limit~~ | UWORD | Not used on peripheral controller (hard coded). Not used on System Controller. |
| ~~prepack\_motion\_count~~ | UWORD | Prepack only. As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~initialize\_zero\_time~~ | UWORD | A-D initialize time? As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~auto\_zero\_time~~ | UWORD | The time the weight must be stable before a new zero can be captured. As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~rate\_option\_limit~~ | UWORD | Not used? |
| ~~zero\_reference\_limit;~~ | UWORD | As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~calibration\_reference\_limit;~~ | UWORD | As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~small\_motion\_limit;~~ | UWORD | Count change above this value indicates “small motion”.  As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~large\_motion\_limit;~~ | UWORD | Count change above this value indicates “large motion”.  As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~large\_motion\_count;~~ | UWORD | Time interval to look for “large motion”. As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~small\_motion\_count;~~ | UWORD | Time interval to look for “small motion”. As far as I can tell, this parameter is never changed (either through UI or calibration) |
| ~~no\_motion\_count;~~ | UWORD | Time there has to be no motion before leaving the "small motion" state. As far as I can tell, this parameter is never changed (either through UI or calibration). |
| ~~zero\_tracking\_option;~~ | UWORD | Not used? |
| ~~negative\_weight\_option;~~ | UWORD | Not used? |
| ~~powerup\_maintenance\_zone\_limit;~~ | UWORD | Not used |
| ~~operate\_maintenance\_zone\_limit;~~ | UWORD | Not used |
| filter\_speed; | UBYTE | Configures filter for SLOW, NORMAL, or FAST. Can change in service screen |
| ~~reference\_voltage;~~ | UBYTE | Not used in Access USB Wgr or HLX |
| last\_calibration\_date; | ULONG | Used to implement the Category1 Audit Trail in the production HLX code. Not needed if replaced by Cat3 Audit Trail. |
| number\_of\_calibrations; | UWORD | Used to implement the Category1 Audit Trail in the production HLX code. Not needed if replaced by Cat3 Audit Trail. |
| ntep\_cc[NTEP\_CCSIZE]; | UBYTE | (NTEP\_CCSIZE = 8). Contains the NTEP number. |
| calibration\_gain\_coefficient; | ULONG | 7730 A-D Register value that’s set at calibration, stored in EEP, and loaded into 7730 on power up. |
| calibration\_offset\_coefficient; | ULONG | 7730 A-D Register value that’s set at calibration, stored in EEP, and loaded into 7730 on power up. |
| weigher\_type; | UBYTE | Primary or Secondary. Set in service screen. |
| load\_cell\_id; | UBYTE | Not used in HLX. Could be used to allow service man to enter loadcell used. |
| flags; | UBYTE | Used by System Controller, stored in EEP. Bit 0 = Weigh Mode (metric/avoir), Bit 1 = DUALRANGE\_NETWEIGHTLIMITCHECK or DUALRANGE\_GROSSWEIGHTLIMITCHECK |
| min\_weight\_to\_print; | LINT | Entered via Service screen |
| weigher\_model; | WeigherModel | Entered via Service screen |
|  |  |  |

1. UBYTE = 1 byte, UWORD, UINT, WeigherModel = 2 bytes, LINT, ULONG = 4 bytes
2. The Access (Atmel) Weigher Code has a better description of all these parameters than the HLX code does.

## Process

* Whenever the software is updated, the new software version must be recorded in the event log.
* Whenever the weighing parameters are changed by the user, the changes must be recorded in the event log.
* Whenever the scale is calibrated all parameters that change as a result of the calibration must be recorded in the event log.

# Other Possible Approaches

## Remote SW update, but no remote Configuration/Calibration?

* Per HB44, a Cat3 Audit Trail is required for “Remote Configuration Capability” (Since SW “handles” the configuration, it’s included in this category).
  + What if Software Update was the only thing that could be done remotely (i.e. weigher configuration parameters couldn’t be modified remotely – and of course the scale can’t be calibrated remotely)? In that case, could we use a Cat1 Audit Trail for Weigher Configuration/Calibration and a Cat 3 Audit Trail for software updates? If yes, it’s possible the Cat3 Audit Trail could be squeezed into the Serial EEP (but it would be close).

## Centralized Event Logger

* Per Pub14 (page DES-134) a “Centralized Event Logger” is allowed. A Centralized Event Logger has an event log for every device (scale) on the network. I envision this being a PC running a software application (add this functionality to HCT?).
  + The advantage of the Centralized Event Logger would be that we wouldn’t have to store the event log on the scale.
  + The disadvantage/caveats are:
    - Whatever program that is the “Event Logger” would be subject to NTEP approval.
    - Pub 14 states: “if the audit trail unit is disconnected or inhibited, the attached network device shall be inoperable and impossible to adjust electronically when in the network configuration”
      * I believe the intent of that paragraph is that the software can’t be updated or the scale configuration changed if the “Central Event Logger” isn’t functional. However the way it’s worded seems to imply the scale has to be inoperable when the “Central Event Logger” isn’t functional.