Evaluación de software en el ámbito de la metrología legal

Software evaluation in the field of legal metrology

Ing. Gustavo Escudero
Instituto Nacional de Tecnología Industrial (INTI) - Electrónica e Informática
E-mail: tavo@inti.gob.ar

Resumen: Dentro del marco establecido por el Programa de Metrología Legal del INTI, el Centro de Electrónica e Informática cumple el rol de laboratorio de verificación y validación de equipos electrónicos como parte del proceso de aprobación de modelo.
En este trabajo se presenta la experiencia del Centro INTI-Electrónica e Informática en el área de evaluación del software embebido en medidores de energía eléctrica activa.
En este documento se describen también, los criterios utilizados para definir la metodología de evaluación a emplear y los puntos críticos que son considerados en la misma.

Palabras clave: medidor de energía eléctrica, evaluación de software, metrología legal.

Abstract: Within the framework established by the Legal Metrology Program of INTI, the Electronics and Informatics Centre fulfills the role of laboratory of verification and validation of electronic equipment as part of the model approval process.
This paper presents the experience of the Centre INTI-Electronics and Informatics in the field of embedded software evaluation of electrical energy meters.
This document also describes the criteria used to define the methodology of evaluation to be employed, and the critical points considered in it.

Keywords: electrical energy meter, software evaluation, legal metrology.

1. INTRODUCCIÓN

Al ser el INTI el organismo oficial responsable de las actividades de metrología legal y a partir de la aprobación del reglamento técnico y metrológico para los medidores de energía eléctrica [1], surgió el requisito de evaluar el software embebido *(firmware)* de estos dispositivos como parte de los ensayos de aprobación de modelo.

Dicha evaluación se debe realizar desde el punto de vista de seguridad, lo que implica verificar que estén implementados los mecanismos de protección necesarios, para evitar la modificación en forma indeseable tanto del *firmware* legalmente relevante como de los parámetros que afecten a la medición.

Se debe tener en cuenta que una falla de seguridad puede dar lugar a que se produzcan

modificaciones indeseables causadas intencionalmente o accidentalmente.
Las modificaciones de origen intencional son aquellas vinculadas directamente al fraude, mientras que las de origen accidental se deben a influencias físicas impredecibles, efectos causados por las funciones de usuario o defectos residuales del *firmware* que pudieran producirse por un diseño incorrecto.
Partiendo de esta base, al definir el proceso de evaluación, el primer paso consistió en determinar la metodología adecuada para este tipo de dispositivos electrónicos, para luego pasar a definir el conjunto de ensayos a realizar.

2. DETERMINACIÓN DE LA METODOLOGÍA DE EVALUACIÓN

Para determinar la metodología de evaluación del *firmware* de un dispositivo electrónico, es necesario definir el nivel adecuado del análisis a realizar. En la práctica existen distintas alternativas que van desde analizar el dispositivo como una caja negra, hasta analizar el código fuente que dará origen al código binario que será embebido en el dispositivo.
Entre estas dos alternativas, existe un abanico de posibilidades que pueden adoptarse para realizar la evaluación. Cada una de ellas implica distintos grados de profundidad y complejidad de análisis y por lo tanto un mayor o menor grado de experticia en el personal técnico actuante, distintos tiempos de ejecución y costos.

Acorde a normativa internacional [2,3] y analizando cómo se realiza este tipo de evaluación en otros institutos de la región, se optó por utilizar el concepto de *clase de riesgo*, ya que al asignar una *clase de riesgo* al instrumento de medida quedan determinados los requisitos particulares de evaluación del *firmware* que deben aplicarse.

Se entiende por *clase de riesgo* a la combinación de los niveles adecuados requeridos de:

a. **Protección del software**: establece que nivel de protecciones deben estar implementadas para hacer frente a los distintos niveles de ataques posibles.
b. **Examen del software**: establece que nivel de análisis y verificaciones deben realizarse.
c. **Conformidad del software**: establece que grado de similitud deben tener los equipos que son instalados en campo con respecto al que se evaluó en el proceso de aprobación de modelo.

Para los medidores de energía eléctrica activa se adoptó una *clase de riesgo* de nivel medio lo que implica que:

a. El *firmware* debe estar protegido frente a cambios realizados intencionalmente utilizando herramientas de software simples, comunes y fácilmente disponibles.
b. Se deben realizar las comprobaciones funcionales estándar del examen de modelo del instrumento y el *firmware* se debe examinar según su documentación.
   Para verificar la fiabilidad de la documentación y la eficacia de las medidas de protección, se deben realizan comprobaciones prácticas aleatorias de las funciones declaradas.
c. La funcionalidad del *firmware* implementado en cada uno de los instrumentos individuales deberá ser conforme con la documentación aprobada.
   Partes del *firmware* se definirán como fijas en el examen de modelo, es decir, modificables solamente con la aprobación previa del organismo evaluador. La parte fija será idéntica en cada uno de los instrumentos individuales.

3. PUNTOS A EVALUAR EN MEDIDORES DE ENERGÍA ELÉCTRICA ACTIVA

De lo puntualizado hasta aquí, se desprende que es indispensable verificar las protecciones implementadas para evitar modificaciones indeseables.

También, para brindar robustez al dispositivo, es importante que el *firmware* esté diseñado para poder recuperarse ante fallos de ejecución o pérdida de alguno de sus parámetros.
No menos importante es que exista algún mecanismo para identificar el *firmware* cargado. Esto es de utilidad para las verificaciones periódicas posteriores a la aprobación de modelo, ya que permitirá detectar en campo si el *firmware* ha sido modificado.

Resumiendo, los puntos a evaluar son:

1. Protección del *firmware* y de los parámetros legalmente relevantes frente a modificaciones fraudulentas.
2. Protección del *firmware* y de los parámetros legalmente relevantes frente a modificaciones accidentales o no intencionales.
3. Recuperación del dispositivo ante fallos.
4. Identificación del *firmware* cargado en el dispositivo.

A continuación se detalla que se debe analizar en cada uno de estos puntos:

3.1 Protección del firmware y de los parámetros legalmente relevantes frente a modificaciones fraudulentas

En esta parte del ensayo se evalúa la posibilidad de realizar modificaciones inadmisibles sin dejar evidencia mediante las interfaces de comunicación, tanto en forma local o remota.
Para ello se analiza el alcance de todos los comandos que el *firmware* puede interpretar y los procedimientos utilizados para cargar el *firmware* en fábrica y para actualizar el *firmware* en campo.
El mismo concepto se aplica para el menú de la interfaz de usuario. Se prueba la actuación manual o secuencia de actuaciones en teclas o interruptores.

Se verifica además, que para realizar cualquier modificación crítica se requiera autenticación o bien, la necesidad de actuar sobre hardware que se encuentre bajo precinto (p. ej. pulsadores).
En este paso, se verifica que las claves utilizadas sean autenticadas por el medidor y que cualquier modificación crítica quede registrada en un registro de eventos.

3.2 Protección del firmware y de los parámetros legalmente relevantes frente modificaciones accidentales o no intencionales

En esta parte del ensayo se comprueba que se genere y verifique en forma automática una suma de comprobación de los bloques de memoria donde están almacenados el *firmware* y los parámetros relevantes.
Esta suma de comprobación tiene la propiedad de no cambiar si no se modifica la información involucrada en su cálculo. Por lo tanto, calculándola periódicamente sobre los mismos bloques de memoria y comparándola con el valor original se pueden determinar inconsistencias.
Para este caso se verifica qué tipo de suma de comprobación se utiliza (CRC, checksum, etc.), con qué periodicidad se verifica la consistencia y cómo indica el medidor la detección de una inconsistencia.

3.3 Recuperación ante fallos

En caso de producirse una falla no intencional es deseable que el dispositivo se recupere adecuadamente de esta condición.
En esta parte del ensayo se verifica que el dispositivo tenga implementado mecanismos de copias de resguardo de parámetros, control de flujo del *firmware*, etc.

3.4 Identificación del firmware

Como se indicó anteriormente, es indispensable que el firmware legalmente relevante esté claramente identificado.
En esta parte del ensayo se verifica que la identificación del *firmware* sea fácilmente visualizable para verificación o inspección, y que dicha identificación esté inequívocamente ligada al *firmware*.
Una forma aceptable de garantizar esta vinculación es que sea el propio *firmware* quien

muestra su identificación, ya sea en la pantalla del equipo o por medio de sus interfaces de comunicación como respuesta a un comando.
No sería adecuado que dicha identificación se indique en la placa de marcado del equipo, ya que el *firmware* podría haber sido modificado pero no así el marcado.

4. CASO PRÁCTICO DE EVALUACIÓN

A continuación, y a modo de ejemplo, se presenta la evaluación de un medidor de energía eléctrica trifásico a 4 hilos, 3x58/100…277/480V, 1(6)A, 50Hz.

Como primer etapa del proceso se evaluó la seguridad frente a modificaciones fraudulentas.
Del análisis de la documentación técnica presentada se determinó que el equipo posee las siguientes interfaces de comunicación:

- Una interface óptica externa para recolección de datos y configuración.
- Una interface serial RS232 interna para recolección de datos, protegida por la envolvente bajo precinto.

Se analizaron y evaluaron funcionalmente los comandos aceptados por dichas interfaces obteniéndose como resultado:

- Ningún comando disponible permite modificar el *firmware* legalmente relevante.
- Los comandos disponibles que no requieren autenticación sólo permiten realizar recolección de datos.
- Los comandos utilizados para operaciones básicas de servicio técnico requieren la actuación sobre un pulsador precintado y autenticación con clave.
- Los comandos que permiten realizar modificaciones de parámetros críticos requieren la apertura de la envolvente, la actuación sobre un pulsador interno y autenticación con clave.
- El medidor se bloquea por 24 horas luego de 15 intentos fallidos de autenticación. El tiempo de bloqueo y la cantidad de intentos fallidos son configurables.
- Las claves son autenticadas por el medidor.

La misma operatoria se empleó con la interface de usuario verificándose que sólo permite la visualización de datos y parámetros pero no su modificación, como tampoco la modificación del *firmware* legalmente relevante.

Como conclusión de esta etapa se determinó que tanto el firmware como los parámetros legalmente relevantes están protegidos frente a modificaciones fraudulentas.

En la siguiente etapa se evaluó la seguridad frente a modificaciones no intencionales.
Analizando la documentación técnica se determinó que la integridad del *firmware* y de los parámetros legalmente relevantes se verifica utilizando una suma de comprobación tipo *checksum*. En ambos casos dicha verificación se realiza al encender el medidor y cada 24 horas en funcionamiento normal.
En caso de detectarse una inconsistencia se indica un mensaje de error en la pantalla del mismo.

Como conclusión se determinó que tanto el firmware como los parámetros legalmente relevantes están protegidos frente a modificaciones no intencionales.

A continuación se evaluaron los mecanismos de recuperación ante fallos, obteniéndose los siguientes resultados:

- Como método de recuperación ante fallos del *firmware* el medidor tiene implementado un mecanismo de control de flujo tipo *watchdog*.
- Para la recuperación ante pérdida de parámetros, el medidor tiene implementado un mecanismo de copia de

seguridad. Al detectarse una inconsistencia los parámetros son restablecidos desde dicha copia.

Como conclusión de esta etapa se determinó que el medidor tiene implementados mecanismos adecuados de recuperación ante fallos.

En la etapa final del proceso de evaluación se verificó mediante análisis de la documentación técnica y con pruebas funcionales que el *firmware* muestra en la pantalla del medidor su número de versión.

Por lo tanto, dado que es el mismo firmware quien muestra su identificación, se puede concluir que ambos están inequívocamente vinculados.

Del conjunto de resultados obtenidos en las distintas etapas del proceso de evaluación se determinó que el dispositivo bajo ensayo cumple con lo solicitado en el correspondiente reglamento técnico.

5. CONCLUSIÓN

La tarea del INTI en el área de evaluación de software de medidores de energía eléctrica impacta positivamente en distintos aspectos.
En el ámbito local, mediante el asesoramiento y la asistencia técnica brindada, logra el fortalecimiento de las empresas proveedoras que obtienen equipos más competitivos y adecuados a los estándares solicitados.
En el ámbito regional impulsa a la vinculación con otros institutos de la región que realizan tareas similares, con el objetivo de intercambiar experiencias y tender a la armonización de las regulaciones.
Esto redunda en un abastecimiento del mercado con equipos funcionalmente más robustos, eficientes y menos vulnerables al fraude lo cual beneficia a la sociedad en general.

Referencias

[1]Reglamento técnico y metrológico para los medidores de energía eléctrica activa en corriente alterna, Resolución 90/2012, Secretaría de Comercio Interior, (2012).

[2] WELMEC 7.2, European cooperation in legal metrology, WELMEC, Software Guide (2009).

[3] OIML D 31, OIML, General requirements for software controlled measuring instruments, (2008)