La controvertida UNE – EN 62676.

Tal y como establece la Orden Ministerial INT/316/2011 en su artículo 3, relativo a la aprobación de material de seguridad privada para ser comercializado y ser utilizado en los servicios de seguridad privada, *"cualquier elemento o dispositivo que forme parte de un sistema de alarma de los recogidos por la normativa de seguridad privada, deberá cumplir, como mínimo, el grado y características establecidas en las Normas UNE-EN 50130, 50131, 50132, 50133, 50136 y en la Norma UNE CLC/TS 50398, o en aquellas otras llamadas a reemplazar a las citadas Normas, aplicables en cada caso y que estén en vigor"*.

Cuando nos referimos a sistemas de alarma contra intrusión la familia UNE–EN 50131-X, recoge por un lado los distintos detectores de interior, como los de infrarrojos pasivos (UNE–EN 50131-2-2), los detectores de microondas (UNE–EN 50131-2-3), los detectores combinados de infrarrojos pasivos y microondas (UNE–EN 50131-2-4), los detectores combinados de infrarrojos pasivos y ultrasónicos (UNE–EN 50131-2-5), los contactos magnéticos (UNE–EN 50131-2-6) y los detectores de rotura de cristal (UNE–EN 50131-2-7), y por otro lado recoge las centrales de alarma y señalización (UNE–EN 50131-3), los dispositivos de advertencia (UNE–EN 50131-4) y las fuentes de alimentación (UNE–EN 50131-6).

De esta manera podemos configurar una instalación de sistemas de detección de intrusión en interiores, utilizando elementos normalizados y por lo tanto potencialmente certificables, en la gran mayoría de los casos, con la significativa excepción de los detectores sísmicos cuya norma correspondiente continúa en fase de elaboración a día de hoy. Sin embargo cuando lo que se pretende es la protección en exteriores (sistemas perimetrales) la ausencia de normas para la selección de elementos es absoluta, disponiendo solo en estos casos de la norma (CLC/TS 50131-7), que no obstante constituye una valiosa guía de aplicación para la instalación de sistemas de intrusión, tanto en interiores como en exteriores, con el menor número de alarmas indeseadas posibles. Para ello proporciona consejos relativos al diseño, a la instalación, al mantenimiento e incluso a la operación de dichos sistemas.

La CLC/TS 50131-7, no es por lo tanto una Norma que posibilite la normalización y posterior certificación de los distintos elementos a utilizar, sino una guía o especificación técnica que pretende garantizar la existencia de sistemas de detección de intrusión fiables y eficaces.

De acuerdo a la UNE-EN 50131-1 los sistemas de detección contra intrusión podrán adoptar distintos grados de seguridad en función de la esperada cualificación de los posibles intrusos. Según la clasificación establecida el grado de seguridad más bajo (grado 1) supondría que los intrusos poseerían muy escasos conocimientos de los sistemas instalados y que en su ataque solo utilizarían por tanto unas limitadas herramientas de fácil adquisición. Por el contrario el grado de seguridad más alto (grado 4), estaría previsto para usar en los casos en los que fuera previsible el ataque por intrusos con conocimientos, habilidades y recursos suficientes para evadir e incluso sabotear los distintos componentes del sistema de intrusión.

Paralelamente desde la citada Orden Ministerial INT/316/2011, en su artículo 2, se incorporan dos nuevos criterios en la graduación de la seguridad de los sistemas, incluyendo por un lado la naturaleza y características del lugar a proteger y por otro la obligatoriedad o no, de conectar dichos sistemas con una central receptora de alarmas o con un centro de control. Se establecen por tanto

otros cuatro grados de seguridad que se hacen corresponder con los existentes en la UNE-EN 50131-1, de manera que:

El grado 1 de la citada norma se corresponde con los sistemas de Grado 1, o bajo riesgo, que serán sistemas que no se van a conectar a una central receptora de alarmas o a un centro de control

Los de Grado 2, de riesgo bajo a medio, serán dedicados a viviendas y pequeños establecimientos, comercios e industrias en general, que pretendan conectarse a una central de alarmas o, en su caso, a un centro de control.

Los de Grado 3, de riesgo medio/alto, destinados a establecimientos obligados a disponer de medidas de seguridad, de acuerdo a lo establecido por el Real Decreto 2364/1994 ó al reglamento de próxima aparición de la vigente Ley 5/2014, así como a otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o, en su caso, a un centro de control.

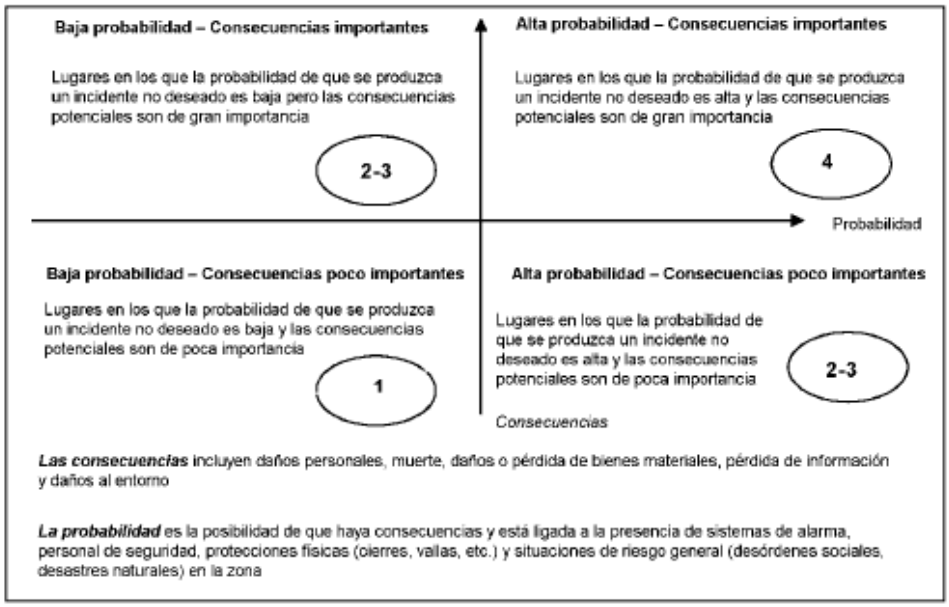
Por último los de Grado 4, considerado de alto riesgo, reservado a las denominadas infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado, y empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos, requeridas, o no, de conexión con central de alarmas o, en su caso, a centros de control.

Los cuatro grados establecidos tanto en la UNE-EN 50131-1 como en la Orden Ministerial INT/316/2011, podrán correlacionarse de manera biunívoca, de manera que el grado establecido en una de ellas pueda ser adoptado por la otra.

Desde el pasado mes de Diciembre, la norma EN 50132-1:2010, referente a los Sistemas de Vigilancia CCTV para uso en aplicaciones de seguridad, ha sido sustituida y actualizada por la UNE-EN 62676-1-1:2015 aunque no será de obligado seguimiento hasta dentro de treinta meses. (Junio de 2019)

La nueva norma UNE-EN 62676-1-1:2015 empieza por renombrar, acertadamente, los hasta ahora denominados Circuitos Cerrados de Televisión (CCTV) por Sistemas de Videovigilancia (VSS, por sus siglas en inglés, *Video Surveillance Systems*) y recoge los requisitos mínimos que debe cumplir un sistema (VSS) que vaya a formar parte de un sistema de seguridad conectado a una Central Receptora de Alarmas (CRA) o a un centro de control. Debemos entender por tanto que esta nueva norma, tiene una directa relación con la Seguridad, y que por ello debe tener una lógica consecuencia en su incorporación a la legislación de seguridad privada.

Al igual que ocurre en el diseño de un sistema de detección de intrusión, los resultados de la necesaria evaluación del riesgo deben utilizarse para determinar los requisitos del Sistema de Videovigilancia (VSS) y de sus distintos componentes y por ende el grado de seguridad a adoptar por el VSS. Los grados establecidos para el VSS en la norma UNE-EN 62676-1-1:2015 se han configurado teniendo en cuenta el nivel de riesgo dependiente de la probabilidad de que se produzca un incidente y del daño potencial causado por él, como se muestra en la figura anexa extraída de la citada Norma.



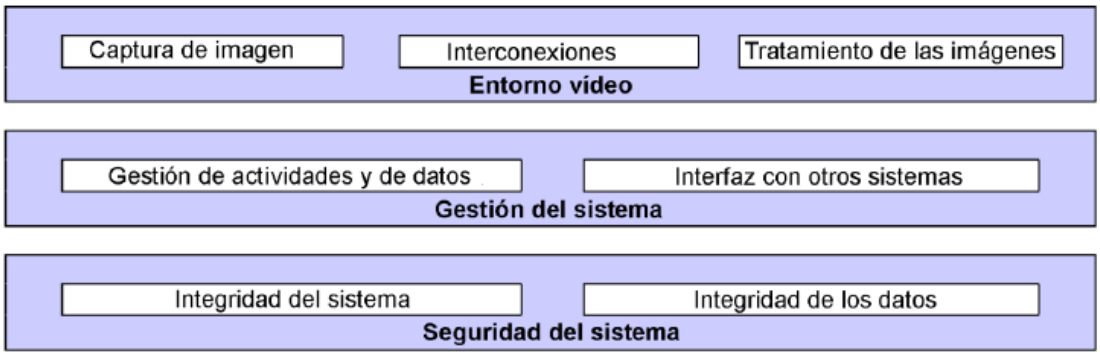
Al confrontar los niveles de riesgo establecidos en la Orden Ministerial INT/316/2011, la UNE-EN 50131-1 y la nueva UNE EN 62676-1-1:2015, nos encontramos con un importante escollo dado que los criterios no son exactamente intercambiables ni biunívocos.

Es necesario por tanto convenir la correlación de todos ellos de manera que:

Criterio	Nivel 1	Nivel 2	Nivel 3	Nivel 4
OM INT/316/2011	Bajo riesgo, no conectables a una central receptora de alarmas o a un centro de control	Riesgo bajo a medio, serán dedicados a viviendas y pequeños establecimientos, comercios e industrias en general, conectados a una central de alarmas o a un centro de control.	Riesgo medio/alto, destinado a establecimientos obligados a disponer de medidas de seguridad u otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o a un centro de control.	Alto riesgo, reservado a las denominadas infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado, y empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos,
UNE EN 50131-1	Bajo riesgo: Intrusos con conocimientos muy escasos de los sistemas de seguridad y con herramientas muy limitadas	Riesgo bajo a medio: Intrusos con conocimientos limitados de los sistemas de seguridad y con herramientas generales e instrumentos portátiles.	Riesgo Medio a Alto: Intrusos con conocimientos de los sistemas de seguridad y con herramientas y equipos electrónicos portátiles.	Riesgo Alto: La seguridad es prioritaria sobre todos los factores. Los intrusos conocen los sistemas y disponen de recursos para planificar la intrusión con una gama completa de equipamiento para evadir o incluso sabotear los sistemas
UEN EN 62676-1	Baja Probabilidad y Consecuencias poco importantes	Alta Probabilidad y Consecuencias Poco Importantes	Baja Probabilidad y Consecuencias importantes	Alta probabilidad y Consecuencias importantes.

Sin embargo y a diferencia de la familia UNE–EN 50131-X, la UNE EN 62676-1, establece ya en su introducción que no tiene como objetivo su utilización para someter a ensayo a los componentes individuales de un VSS. No podremos esperar por tanto de ella la normalización de los distintos componentes ni como consecuencia, su posible certificación.

Tal y como expone la Norma podemos definir un sistema de Videovigilancia (VSS) como un conjunto de partes funcionales y las relaciones que existen entre ellas. Un Vss utilizado en aplicaciones de seguridad se puede presentar en bloques funcionales que describen las distintas partes y funciones del sistema según la figura anexa extraída de la citada Norma.



El diseño de un adecuado VSS no dependerá tanto de la utilización de un equipamiento concreto con unas características determinadas sino de la funcionalidad que proporciona al sistema de seguridad para el que está concebido. Estas funcionalidades no son intrínsecas a un componente del sistema ni siquiera a uno de los tres entornos expuestos (Entorno de Vídeo, Gestión del Sistema y Seguridad del Sistema), incluso un único dispositivo podrá realizar varias funciones. Una cámara de televisión podrá, por ejemplo, capturar las imágenes, almacenarlas temporalmente, analizarlas y procesarlas e incluso transmitirlas para su envío a través de la red.

Consecuencia de todo ello y de la imposibilidad de normalizar el distinto equipamiento para su instalación con determinado grado de seguridad, lo que la norma 62676 en su parte 4 expone, son directrices de aplicación y establece una lista de diez y ocho funcionalidades, que conformarán los criterios a tener en cuenta para definir el grado de seguridad de un VSS.

La funcionalidades establecidas son: las Interconexiones comunes, la capacidad de Almacenamiento, el Archivado y copia de seguridad, La Información relacionada con la alarma, los Registros del sistema, la Copia de seguridad y la restauración de los datos del sistema, la Notificación de fallo repetitivo, la protección contra la manipulación de imágenes, el Tiempo de espera del búfer de imagen, las Funciones esenciales de fallo de un dispositivo y el tiempo de notificación, el Monitoreo de interconexiones, la Detección de manipulaciones, los Requisitos de código de autorización, la Sincronización de tiempos, la Autenticación de datos, la Autenticación de exportación / copia, el Etiquetado de datos y la Protección de datos (manipulación)

La norma UNE-EN 62676-1-1:2015 proporciona un nuevo enfoque global para los sistemas de video vigilancia en contrapunto a las tradicionales normas de producto, definiendo el uso de “buenas practicas” y un conjunto de instrucciones con las que garantizar:

- que las necesidades de un usuario potencial estén debidamente especificadas y entendidas.

o que el sistema esté diseñado, instalado, operado y mantenido para satisfacer las necesidades del usuario:

- Permitiendo la comparación entre las propuestas de los proveedores.
- Permitiendo la aplicación coherente de las funciones.
- Proporcionando un método simplificado para especificar un sistema.

De esta manera las distintas funcionalidades descritas podrán ser exigibles o no, en mayor o menor medida, en función del grado de seguridad que se haya asignado al sistema, pudiendo incluso disponer de un sistema con un grado de seguridad superior en alguna de las funcionalidades o incluso inferior si aquella funcionalidad en concreto no fuera precisa.

Podremos tener recomendaciones de grado para cada una de las funcionalidades, y el grado de la instalación será aportado por el diseñador de la instalación en primer término y del instalador posteriormente. El requisito de que un elemento o componente individual sea capaz de satisfacer una funcionalidad especificada en la norma no es fácil, dado que cómo hemos expuesto esta funcionalidad podrá ser aportada por varios de los elementos elegidos en cualquiera de los tres entornos definidos o incluso suponiendo que un elemento pudiera aportar los requerimientos para posibilitar una funcionalidad en un grado determinado, este dependerá del sistema en el que vaya instalado.

Existirán no obstante ciertos requerimientos relevantes que un producto no será capaz de cumplir en un grado superior, esta circunstancia sí limitará claramente ese producto concreto sin importar lo que el resto del sistema aporte.

Debemos entender por tanto que a pesar de la regulación establecida por la OM INT 316/2011 para la adopción y certificación del grado de seguridad en los sistemas de Videovigilancia (VSS), la normalización aportada por la UNE –EN 62676 no posibilita la certificación de componentes o productos individuales, sino la regularización de determinadas funcionalidades y su grado de cumplimiento en función de los niveles de seguridad en ella establecidos.

De esta misma opinión es la British Security Industry Associations (BSIA) según se desprende del análisis de los documentos publicados en su web (www.bsia.co.uk). Form 217 – BS-EN 62676 series – Guidance for customers about grading and other important matters and Form 218 – Grade requeriments under BS EN 62676 standard for CCTV)

En este contexto surge la necesidad de concretar, cómo y quién debe certificar una instalación de Videovigilancia y el papel que en ello deben representar las figuras de Técnico e Ingeniero indicadas en la Ley 5/2014 como personal Acreditado según se expone en su artículo 19.1.c y en el artículo 46.1, y salvando lo indicado en el artículo 52.2.

La controversia está servida.

Julio Pérez Carreño
Director de Departamento de Eulen Seguridad, S.A.
Secretario de la Junta Directiva de AES.
Coordinador del Grupo de Seguridad Electrónica de AES