

7. Sistema de Gestión de Datos de Medida

El modelo genérico de un MDM (Meter Data Management) es similar al indicado en la Fig. 15, que se corresponde con el sistema implantado por la distribuidora Acea en Italia [38].

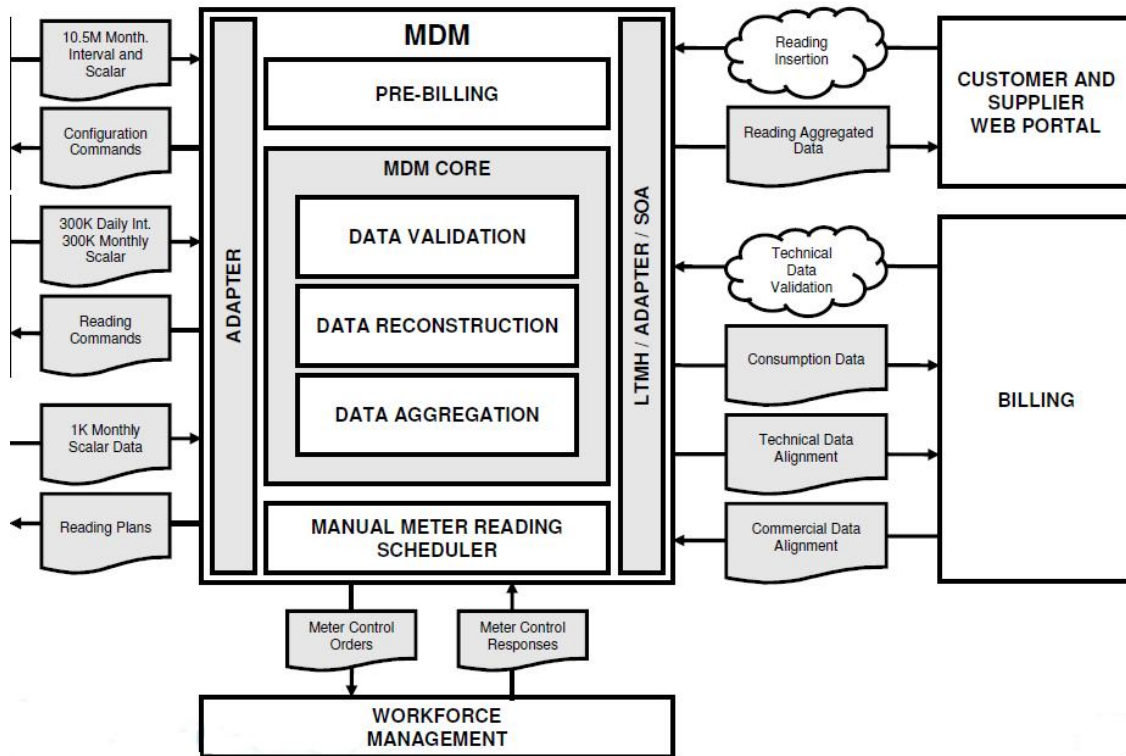


Fig. 15: Modelo de MDM

El MDM recibe las diferentes lecturas de los concentradores. Cuando los datos recibidos son almacenados por parte del sistema de gestión, se realizan una serie de funcionalidades comunes, independientemente del modelo implementado:

- Proceso de validación de las lecturas.
- En los casos que se detecte un error en la lectura:
 - Se realiza una estimación de la misma en base a los valores históricos.
- Agregación de los resultados para su presentación.
- Almacenamiento de los datos y envío tanto al sistema de facturación

como a otros sistemas que requieran los datos según se indicó en apartados anteriores.

- El sistema dispondrá de herramientas para la minería y análisis de los datos.
- La gestión de la red estará integrado y será en encargado de recibir y enviar los diferentes eventos a los contadores.
- Comunicación con otros sistemas de gestión.

Además de las funcionalidades indicadas el sistema debe ser diseñado en la medida de lo posible con las siguientes características:

- Debe ser fácilmente escalable. El sistema debe soportar un gran volumen de información ya que deberá almacenar curvas de consumo mensuales y un histórico para que esté accesible para los implicados.
- Debe ser un sistema flexible al que se le puedan configurar nuevos requerimientos y se pueda adaptar a los cambios en el marco regulatorio y a los propios del negocio.
- Para permitir un manejo adecuado de esta información debe tener un alto rendimiento, para lo cual deberá por ejemplo aplicar técnicas de paralelismo en el motor de cálculo.

7.1. Seguridad en los Sistemas de Telegestión

Uno de los problemas a los que se enfrenta el desarrollo de los nuevos sistemas de telegestión es la seguridad de los datos y del control de los nuevos contadores (con capacidad para emitir órdenes de corte y conexión de forma remota). Una de las primeras medidas que se toman en el diseño de los datos, es la encriptación de los mismos. Sin embargo, la simple inclusión de la encriptación no es suficiente para asegurar la integridad de la información. Por ello, en el diseño del sistema de telegestión se plantean una serie de cuestiones clave que deben ser gestionadas de manera adecuada [41]:

- **Confidencialidad:** El sistema debe asegurar que los datos sólo son accesibles para las entidades que realmente tienen autorización, evitando en todo momento la divulgación de los datos.
- **Integridad:** No sólo hay que evitar la posible divulgación de los datos, sino también que de forma intencionada se modifique, añada o elimine parte o la totalidad de la información.
- **Disponibilidad:** Los datos deben ser accesibles en todo momento por las entidades autorizadas.
- **Responsabilidad:** Cualquier interesado con obligación a recibir una información no puede negarse a ello, así como un interesado que no debe recibir parte de la información no puede tener poder de decisión para recibirla.

Estas cuestiones deben ser consideradas en todos los bloques definidos en el sistema de telegestión, así como definir las posibles restricciones para una minimización de las mismas.

Confidencialidad

La confidencialidad es uno de los aspectos más valorados por parte de los clientes, que no desean que entidades (empresas o particulares) conozcan sus patrones de consumo eléctrico, ya que a partir de ellos se pueden realizar otro tipo de estudios. Por tanto, estos datos deben ser confidenciales, incluso considerando el robo de los contadores, para un posterior acceso a los datos almacenados.

El sistema deberá asegurar la confidencialidad de la información en los dos canales de comunicación que suelen existir entre el cliente y el centro de procesamiento de los datos. Otro aspecto a destacar es evitar la comunicación cliente a cliente bien a través de la arquitectura, o si esta no lo permite (como en el caso en el que un contador puede actuar como repetidor), a través de medidas de seguridad.

Por último, el sistema de procesamiento de datos debe proveer las medidas de seguridad estándar para los sistemas de información.

Integridad

La integridad en los sistemas de telegestión debe evitar tanto los posibles cambios de datos, como prevenir la integridad de los comandos o eventos de control del sistema. En este sentido, uno de los fallos de integridad más graves podría ser el envío de la señal de desconexión a todos los contadores de una zona o la totalidad del sistema.

Para asegurar la integridad en el contador debe ser protegido tanto física como a nivel lógico. Esto no asegura que el contador pueda ser robado o el chip del contador modificado. Lo que se puede asegurar es que en el momento que el posible “ataque” sea detectado, se apliquen las acciones necesarias, como la desconexión del contador o ignorar cualquier tipo de comando que provenga de él hasta que se determinen las causas.

Como hemos comentado anteriormente, los canales de comunicación son externos y desarrollados en entornos inseguros y accesibles. En este caso, el desarrollo se debe centrar en detectar las posibles violaciones a la integridad con el objeto de prevenirlas.

En el caso del centro de procesamiento, la integridad se deberá centrar en el control de los posibles errores cometidos por descuidos humanos a la hora de la manipulación y además, en los posibles ataques realizados por el propio personal de la compañía, que conoce perfectamente las posibles debilidades del sistema y cómo hacer uso de ellas, con lo que se pueden enviar eventos falsos, conectar o desconectar contadores.

Disponibilidad

La disponibilidad de la medida no ha sido un problema a corto plazo hasta ahora. En los casos en el que la medida no estaba disponible, se realizaba una facturación estimada hasta la obtención de la lectura correcta, en la que se ajustaba el volumen global de consumo y facturación estimada con el real consumido en ese periodo de tiempo. En los casos que este periodo fuese más amplio que el indicado por la legislación correspondiente, se establecían mecanismos para la obtención de una lectura real.

Para los nuevos sistemas de telegestión, esta posibilidad presenta mayores problemas desde el punto de vista que la medida del consumo de los clientes no sólo se utiliza para la realización de una factura. En estos casos, lo que se debe determinar es el tiempo máximo en los que la información de un determinado cliente se puede considerar como no disponible y en la medida de lo posible, detectar las causas de la indisponibilidad.

Además del análisis del posible tiempo máximo de indisponibilidad por parte del sistema, al cliente también afecta estos tiempos, sobre todo si se tienen en cuenta posibles aplicaciones futuras, como puede ser la aplicación de precios a tiempo real.

En el caso de los canales de comunicación, además de los posibles fallos inherentes al sistema de comunicaciones, se debe tener especial cuidado en el diseño de los mismos para el tratamiento de sobrecargas.

Por último, en el caso del sistema de procesamiento de datos, con un diseño adecuado del mismo la disponibilidad deberá ser asegurada.

Responsabilidad

Cuando hablamos de responsabilidad, el principal implicado es sistema de procesamiento de datos, tanto para la recepción de los consumos de los clientes, como para el envío de la información de la facturación y gestión de los eventos de los distintos sistemas debido a que en estos casos están implicados diferentes interesados (distribuidor, comercializador, empresas de gestión de la medida).

Restricciones

A pesar de las consideraciones de seguridad realizadas, existen una serie de limitaciones a la hora de realizar la planificación de las mismas.

Entre las restricciones que debemos imponer al contador podemos destacar principalmente el coste del mismo que limitan los requerimientos de seguridad.

En cuanto a los canales de comunicación, las restricciones pueden venir determinadas por el ancho de banda de ciertas partes del sistema o por el uso de servicios de telecomunicaciones públicos.

Por último, para el sistema de procesamiento de datos las restricciones pueden venir dadas por los accesos que deben hacer otros sistemas.

En el diseño del sistema de telegestión debemos conseguir un compromiso entre las medidas de seguridad que se deben aplicar y las restricciones que tiene el sistema, de forma que se dificulte en el mayor grado posible cualquier intrusión en el mismo.