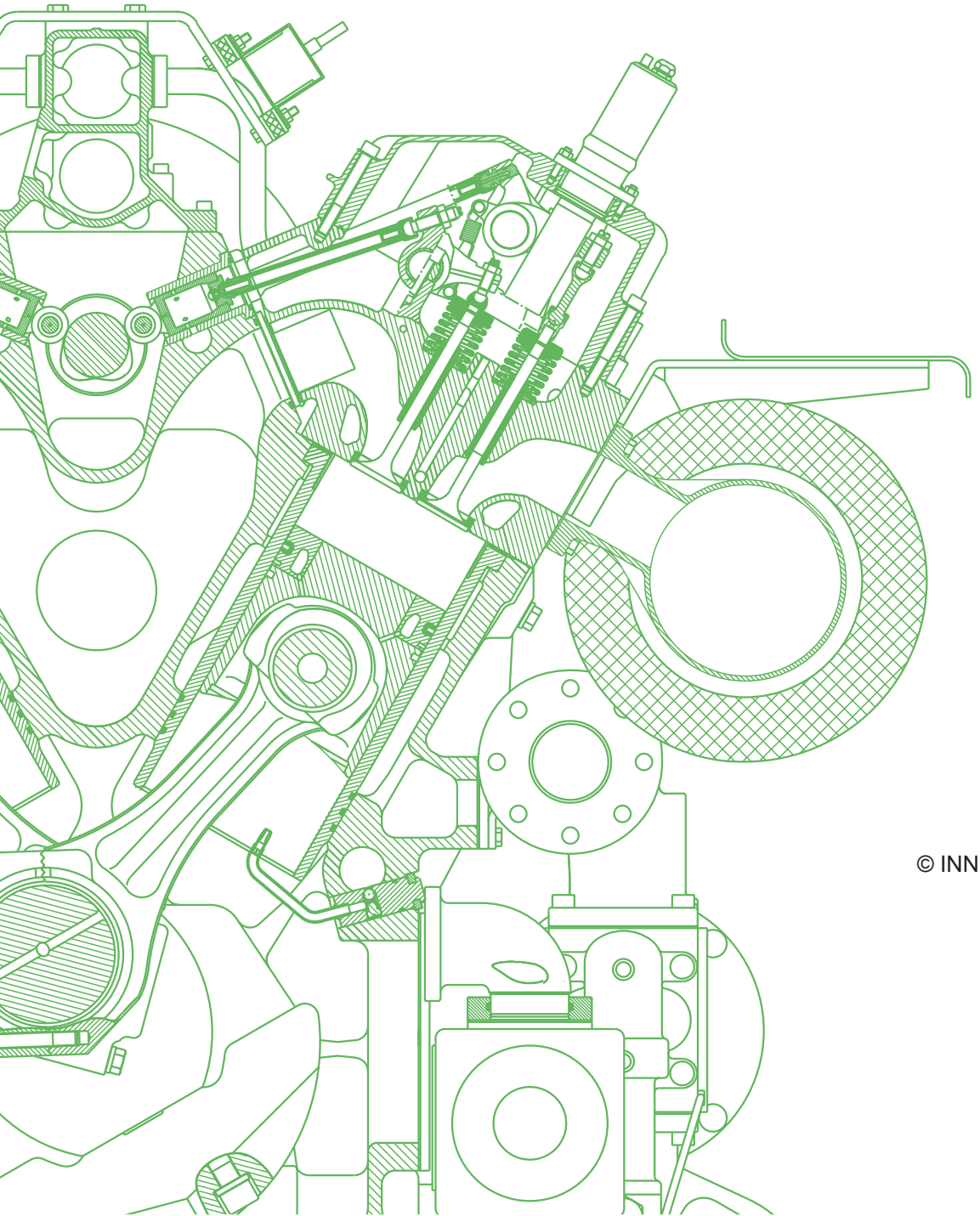
JENBACHER

TA 2300-0006

Instrucción técnica

Indicaciones técnicas de seguridad para el acoplamiento de instalaciones de Jenbacher a internet



Achenseestr. 1-3
A-6200 Jenbach, Austria
www.innio.com

JENBACHER
INNIO

JENBACHER

TA 2300-0006
Indicaciones técnicas de seguridad para el acoplamiento de instalaciones de Jenbacher a internet

Los destinatarios de este documento son:

Clientes, distribuidores autorizados, servicios técnicos autorizados, servicios de puesta en marcha autorizados, filiales, Jenbach HQ

1 Generalidades

Por medio de un enlace a la red, los Sistemas de Servicio DIA.NE ® de INNIO Jenbacher GmbH & Co OG ponen a disposición un acoplamiento con el cliente. Mediante este acoplamiento es posible acceder por medio del navegador web a la Aplicación de Visualización WIN de DIA.NE® y gestionar la instalación.

Este enlace a la red ha sido planificado por INNIO Jenbacher GmbH & Co OG EXCLUSIVAMENTE para la conexión de una red local (cliente - LAN).

Gracias a las tecnologías actuales y a la difusión de las conexiones a internet, tales acoplamientos a la red se prestan por principio también al acceso por medio de internet. Por lo general, esto lo resuelve el cliente por medio de un *router* y habilitación de puertos.

Estas instrucciones técnicas explican los peligros que implica una solución de este tipo, y expone la solución, conveniente desde el punto de vista de la seguridad técnica, de un enlace de las instalaciones de INNIO Jenbacher GmbH & Co OG a internet.

2 Riesgos para la Seguridad / Peligros

Una solución mediante un *router* de internet y habilitación de puertos implica **grandes riesgos para la seguridad**.

Entre otros:

- Transmisión no codificada de los datos en internet
  - Los *HACKERS* pueden averiguar contraseñas transmitidas en texto legible
  - Posibilidad de un ataque *Man-in-the-Middle* (modificación online por los *HACKERS* de los datos transmitidos, como, por ejemplo, valores teóricos prefijados, parámetros, etc.).

- En el caso de una configuración esencialmente correcta del *router* (restringida a puertos determinados): Es posible un acceso directo al servidor web instalado en el servidor de DIA.NE WIN
  - No hay protección contra los ataques de virus y gusanos, de negación de servicio (DoS, *Denial of Service*) y de exploits (por ejemplo, Code Red)
  - Poca protección ante ataques de descifrado de contraseñas por *HACKERS* (determinación de contraseñas)
- En caso de una configuración errónea del *router* o de una ejecución a destiempo de actualizaciones de seguridad: Acceso directo al sistema operativo del servidor
  - No hay protección contra los ataques de virus, gusanos o troyanos en el sistema operativo de Windows (por ejemplo, Blaster, Sasser, Spybot, Beagle, etc.)
  - Los *HACKERS* pueden eludir la protección de contraseñas en todos los niveles
- No hay control ni protocolización de acceso por el Portal de Acceso Remoto de INNIO Jenbacher GmbH & Co OG
  (procedimiento de autenticación de dos capas)

De todo esto resultan los **siguientes peligros inmediatos para el cliente y la instalación**:

- Acceso de una persona extraña a la instalación mediante una contraseña obtenida por espionaje o mediante un ataque *Man-in-the-Middle:*
  De esta manera, y en función del nivel de la contraseña, es posible leer, modificar o borrar la totalidad de los valores nominales, parámetros de motor o datos históricos.
- En el caso que una persona extraña se haga con el control del servidor:
  - Pueden eludirse la totalidad de las disposiciones de seguridad del sistema operativo, y con ello es posible un acceso ilimitado a la totalidad de los valores nominales, parámetros de motor o datos históricos
  - Es posible una utilización del servidor para tareas criminales de otro tipo (correo basura, ataques DoS, etc.).
- Destrucción del servidor de DIA.NE® WIN:
  Fallo total del servidor por borrado de la totalidad de los datos en el disco duro, debido a intervención de *HACKERS* o a un VIRUS.

Estas manipulaciones pueden llevar a la destrucción de la instalación y poner vidas en peligro.

3 Solución mediante el firewall de Jenbacher

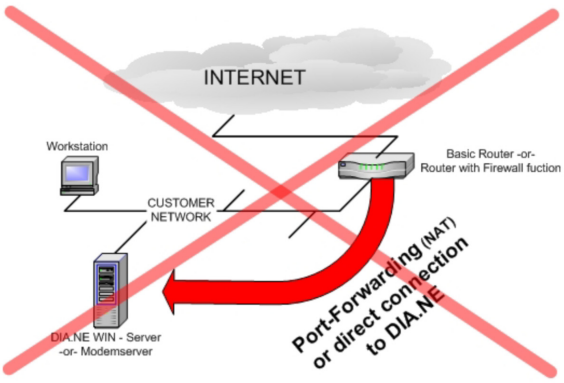
A efectos de subsanar por completo los problemas de seguridad mencionados arriba, INNIO Jenbacher GmbH & Co OG ha desarrollado una solución.

Esta solución consiste en un *firewall* instalado *in situ*, que permite una conexión de alta seguridad y codificada con el *firewall* central en la Central de INNIO Jenbacher GmbH & Co OG (Virtual Private Network, VPN). Esta conexión y los componentes empleados son controlados y mantenidos directamente por INNIO Jenbacher GmbH & Co OG, lo que permite una reacción muy rápida a los problemas de seguridad relacionados con el sistema (actualizaciones de seguridad), así como a las actividades de los hackers.

Gracias al *Firewall* y a la conexión VPN ya no es posible un acceso directo a la instalación desde internet y se asegura solamente un acceso controlado por medio del Portal de Acceso Remoto de INNIO Jenbacher GmbH & Co OG.

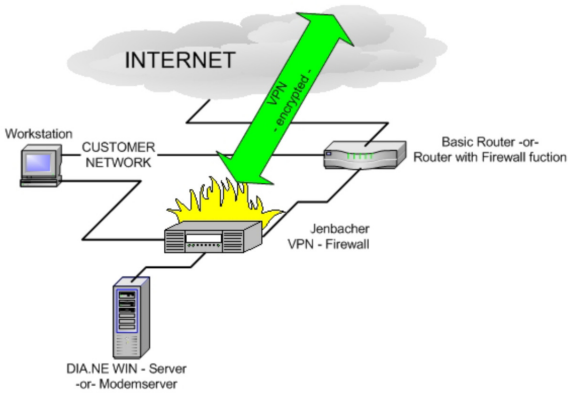
4 Advertencia

TERMINANTEMENTE PROHIBIDO
No seguro



Router con habilitación de puertos:
Acceso directo a DIA.NE® WIN con un inicio de sesión no codificado mediante contraseña de DIA.NE®.

Seguro



Solución de firewall de INNIO Jenbacher GmbH & Co OG**:**
Acceso a DIA.NE® WIN solo mediante Remote Access Portal INNIO Jenbacher GmbH & Co OG (1. autenticación codificada en el portal, 2. inicio de sesión codificado con contraseña DIA.NE®)

INNIO Jenbacher GmbH & Co OG no se responsabiliza por defectos o daños atribuibles a la utilización de un *router* con habilitación de puertos o a una conexión directa al servidor DIA.NE® WIN. Para tales defectos o daños INNIO Jenbacher GmbH & Co OG no asume ninguna garantía.

5 Mención de revisión

Histórico de revisiones

Índice	**Fecha**	**Descripción/Resumen de cambios**	**Experto** *Revisor*
2	30.04.2019	GE ersetzt durch INNIO / GE replaced by INNIO	**Stojiljkovic T.** *Pichler R.*
1	26.05.2010	Umstellung auf CMS / Change to **C**ontent **M**anagement **S**ystem ersetzt / replaced Index: **-**	**Schartner** *Pichler*