Incorporar el análisis de riesgos de los ciberprocesos a la era digital

Ampliación del análisis de riesgos de procesos para abarcar los riesgos cibernéticos.

Por: Hossain Alshedoki and Tim Johnson

El análisis de riesgos de procesos (PHA, por sus siglas en inglés) es una característica establecida en el mundo del petróleo y el gas y de las plantas industriales, que realiza revisiones y correcciones sobre el hardware en las operaciones de las que dependen los procesos. Basado en la metodología de la OHSA 1910.119, el PHA se basa en 14 elementos interrelacionados para crear un programa integral que evite la liberación de materiales peligrosos.[1]

Sin embargo, a medida que el hardware de las redes de las empresas industriales se va haciendo cada vez más tecnológico, con componentes de control de procesos que se comunican entre sí en un dominio de Sistema de Control Industrial (ICS)/Tecnología Operativa (OT), surgen nuevos riesgos que exigen nuevos niveles de PHA. Los componentes del control de procesos ya no son elementos aislados, desconectados de otras partes del dominio ICS o de la red de tecnología de la información (TI). Los requisitos de ICS/OT para interactuar con la TI están produciendo una convergencia cada vez mayor, ampliando las vías y los puntos centrales a través de los procesos críticos del control de procesos. Existe una creciente intersección entre los sistemas de seguridad y los sistemas de control de procesos que da lugar a nuevos vectores de ataque que pueden ser explotados por los ciberatacantes.

Este problema se está volviendo demasiado real. Los incidentes de ataques de ransomware a las redes de OT se han multiplicado, quintuplicándose de 2018 a 2020. De ellos, las entidades del sector manufacturero representaron más de un tercio de los ataques de ransomware confirmados contra organizaciones industriales, seguidas por las empresas de servicios públicos, que representaron el 10%.[2] El costo global estimado de estos ataques de se ha disparado y se ha predicho que alcanzará los 20 mil millones de dólares en 2021, en comparación con los 325 millones de dólares en 2015.[3] La disrupción operativa debida al ransomware en entornos de OT se ha multiplicado por 23. En 2020, hubo un aumento del 32% en los ataques de ransomware contra organizaciones de energía y servicios públicos.[4]

Con el paso del tiempo, los ataques de ransomware se han vuelto más sofisticados y han cambiado para conseguir sus fines mediante diferentes métodos. Además, este tipo de ataques se han dirigido cada vez más a entornos ICS como el petróleo y el gas y la manufactura.

Evolución del ransomware[5]

Ransomware de primera generación

- Se enfocaba en encriptar archivos del sistema y exigir un rescate
- Simple, motivado por los puntos finales

Ransomware de segunda generación

- Enfocado en las vulnerabilidades
- El ransomware desarrolla capacidades de propagación lateral y es wormable
- Altamente enfocado en organizaciones de TI

Ransomware de tercera generación

- Pasa de ser sólo un negocio a una disrupción y exfiltración de datos
- Las técnicas de rescate incluyen el cifrado de datos y la filtración de datos sensibles en línea si no se paga
- Comienzan a aparecer comportamientos similares a los de las APT con un tiempo promedio de detección de 45 días
- Pasa hacia el entorno ICS: petróleo y gas, manufactura, etc.

[1] US Department of Labor, Occupational Safety and Health Administration, 1910.119 — Process safety management of highly hazardous chemicals

[2] Ransomware in ICS Environments, Dragos, December 2020.

[3] Global ransomware damage costs predicted to exceed $265 billion by 2031, Cybersecurity Ventures, June 3, 2021.

[4] Claroty Biannual ICS Risk & Vulnerability Report: 1h 2020, Claroty, 2020.

[5] Asegurar un mundo hiperconectado, KPMG International, 2021

Un panorama de amenazas crecientes

Los ataques de ransomware son sólo una característica de un complejo y cada vez más agresivo panorama de amenazas contra el que las organizaciones deben protegerse. Esto incluye:

Amenazas en evolución

Los ciberdelincuentes se están adaptando, diversificando y comportándose más como agentes estatales. Las operaciones criminales están cambiando sus tácticas para reducir los riesgos de detección y aumentar las disrupciones. Están intentando maximizar el rendimiento de sus esfuerzos de varias maneras, como por ejemplo: dejando de lado las asociaciones para operar dentro de sindicatos muy unidos; aprovechando la mayor disponibilidad de información de los sistemas de información geográfica para iniciar los ataques; aumentando la precisión de los objetivos mediante el uso de documentos legítimos para identificar a las posibles víctimas antes de entregar el malware; o vendiendo y comprando acceso directo a las redes para la entrega de ransomware en lugar de llevar a cabo intrusiones avanzadas.

Ransomware dirigido

Hay una compleja gama de motivos para los ataques de ransomware dirigidos. Aunque la motivación detrás de un ataque puede parecer financiera, también puede haber motivos híbridos: una combinación de motivos financieros, ideológicos y/o políticos. En cualquier caso, estos ataques pueden afectar a la disponibilidad de las infraestructuras ICS/OT. Aunque la amenaza del ransomware sigue existiendo, las organizaciones deben asegurarse de tomar las medidas adecuadas para preparar, prevenir, detectar, responder y contener un ataque de ransomware en toda la empresa.

Amenazas a la cadena de suministro

La mejora de la higiene del ecosistema está empujando a las amenazas hacia la cadena de suministro, convirtiendo a los amigos en enemigos. La interconexión global de las empresas, la adopción más amplia de las contramedidas tradicionales de la industria contra las ciberamenazas y las mejoras en la higiene básica de la ciberseguridad parecen estar empujando a los actores de las ciberamenazas a buscar nuevas vías para comprometer a las organizaciones, como dirigirse a sus cadenas de suministro, incluidas las de software, hardware y la nube.

La vida después de la crisis

Las vulnerabilidades en la infraestructura ICS/OT exigen soluciones ajustadas/objetivadas para evitar el impacto en su disponibilidad. El descubrimiento de vulnerabilidades en el hardware de control de procesos patentado, como los controladores lógicos programables (PLC), en los últimos años, combinado con el uso de software y hardware comercial utilizado para las interfaces hombre-máquina (HMI), las estaciones de trabajo de ingeniería y los sistemas de soporte de ICS, como los historiadores, tienen un impacto en la disponibilidad del sistema, aumentando el riesgo para las organizaciones, lo que podría conducir a la pérdida de vidas.

Geopolítica comprometida

A medida que surgen nuevas amenazas derivadas de la desinformación y la evolución de la tecnología, las empresas globales pueden encontrarse en el punto de mira mientras persisten las tensiones geopolíticas. Los actores de las ciberamenazas no sólo pueden mantener los niveles actuales de actividad, sino también aprovechar las nuevas capacidades a medida que las nuevas tecnologías permiten tácticas, técnicas y procedimientos (TTP) más sofisticados que se centran en los entornos ICS/OT.[6]

[6] Security magazine, Five factors influencing the cyber security threat landscape (2019)

Fortalecimiento de las defensas a través del Cyber-PHA

Como resultado de estos factores, es necesario ampliar el PHA tradicional para proteger el control de procesos realizado en el dominio ICS/OT. Esta necesidad se agudiza porque la comunicación del sistema de seguridad se está integrando en el dominio ICS/OT a medida que estos sistemas se digitalizan y conectan más. Si el sistema de seguridad interconectado está en peligro, la capacidad de controlar un proceso fuera de control se ve comprometida, lo que puede dar lugar a riesgos ambientales y operativos, e incluso a la pérdida de vidas. Además, como los sistemas de control y seguridad convergen cada vez más con los sistemas informáticos, una brecha cibernética en estos últimos podría extenderse también al ámbito de los ICS/OT.

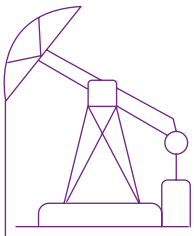
Por eso se necesita un Cyber-PHA adicional, para hacer frente a los riesgos y amenazas cibernéticas que actualmente caracterizan el panorama industrial. Bienvenido al Cyber-PHA.

En un mundo ideal, el primer paso es garantizar que su dominio ICS/OT tenga resiliencia cibernética mediante la segmentación de la red. Esto implica la segmentación de la red en zonas y conductos, y un límite claro entre los dominios de TI y de ICS/OT. Esta es la premisa de la norma IEC 62443, una serie de documentos que orientan sobre la seguridad de ICS/OT. Abarca la orientación general, la política y los procedimientos, la tecnología y el diseño del sistema, así como los requisitos de los componentes. En cualquier caso, independientemente de que exista una segmentación formal de la red, hay que centrarse en reforzar la resiliencia cibernética para que las operaciones puedan seguir funcionando incluso si una amenaza ha penetrado en el perímetro de una red.

Un Cyber-PHA puede ayudar a identificar, verificar y diseñar los límites de los dominios ICS/OT. El Cyber-PHA es una metodología orientada a la seguridad para identificar y evaluar el riesgo cibernético de los dominios ICS/OT y los sistemas instrumentados de seguridad (SIS). Por lo general, sigue una metodología similar a la de un HAZOP (estudio de peligros y operabilidad), pero adaptada para el ciberespacio, que se conoce como CHAZOP.

Un Cyber-PHA suele realizarse en fases, es escalable y puede aplicarse a sistemas individuales o a instalaciones o empresas enteras. Hay seis fases clave:

1. El personal del emplazamiento y el evaluador de amenazas (el equipo de peligros y operabilidad (HAZOP)) deben alinearse y acordar el área de interés que se evaluará.
2. Recopilar información sobre los componentes de OT con la red de OT y el SIS, y sus conexiones para identificar las vulnerabilidades.
3. Analizar los datos y documentar las posibles vulnerabilidades que pueden ser explotadas durante un evento cibernético.
4. Llevar a cabo un curso práctico de Cyber-PHA en el que se reúna, analice e integre la información con escenarios de amenazas para desarrollar un panorama completo de los riesgos.
5. Una vez completado el Cyber-PHA, se elabora un amplio informe que muestra los riesgos para los dominios ICS/OT y SIS, y un plan para mitigar los riesgos hasta el nivel aceptable de la organización.
6. Un plan de reparación eficaz incluye una lista priorizada de acciones, estimaciones presupuestarias, calendario y requisitos de recursos, que en conjunto pueden proporcionar niveles adecuados de resiliencia.



El Cyber-PHA es una **metodología orientada a la seguridad** para identificar y evaluar el riesgo cibernético de los dominios ICS/OT y los sistemas instrumentados de seguridad (SIS).

Un escenario ideal sería que un Cyber-PHA se llevara a cabo poco después de un PHA tradicional, basándose en sus resultados para identificar y abordar los problemas cibernéticos.

El resultado del análisis de peligros y riesgos debe identificar los peligros y vulnerabilidades potenciales, a la vez que proporciona temas de riesgo procesables que facilitan las recomendaciones prácticas para su aplicación. Aunque el panorama de las amenazas a la ciberseguridad cambia continuamente, existen clasificaciones generales de los posibles agentes o fuentes de amenazas que una organización debe tener en cuenta:

1
Ataque externo - técnico

2
Ataque interno - no técnico

3
Uso indebido y abuso interno

4
Acceso no autorizado

5
Compromiso de la información (Logic Mod)

6
Mal funcionamiento del sistema

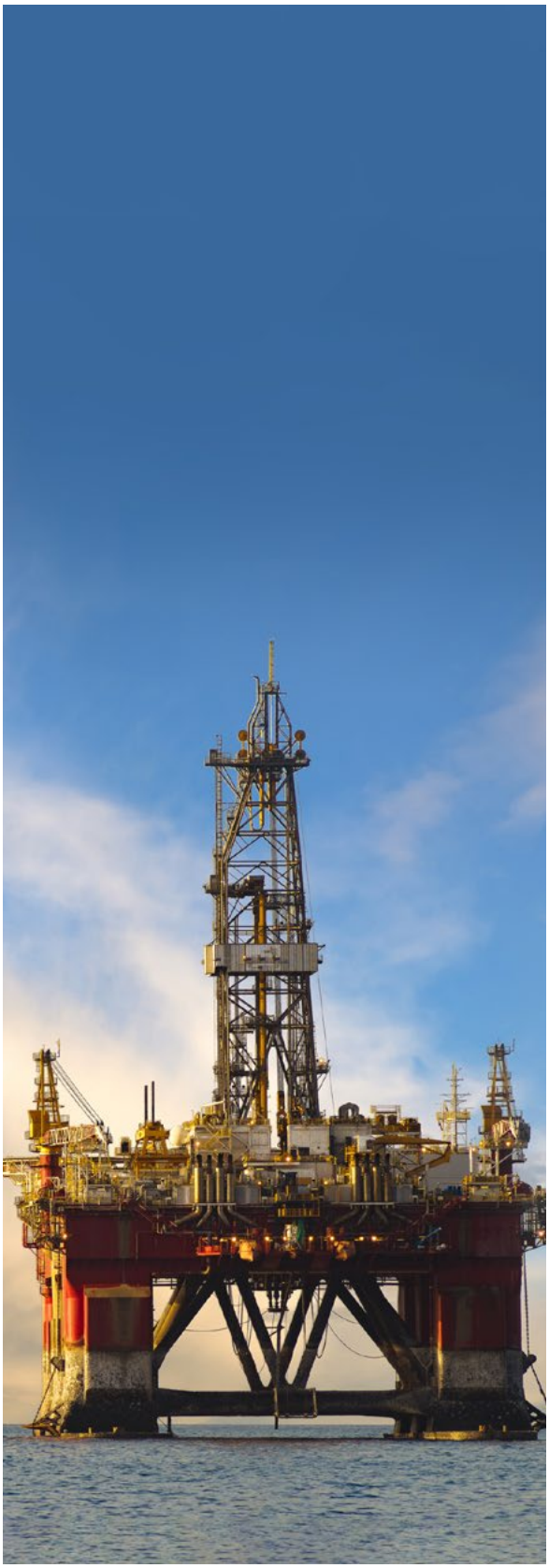
7
Interrupción del proceso

8
Interrupción del sistema de seguridad

9
Error humano

10
Efecto imprevisto de los cambios

Se puede desarrollar una hoja de ruta de ciberseguridad detallada y desglosada en los logros rápidos más importantes resumidos, soluciones múltiples a corto plazo y alineaciones estratégicas a largo plazo para alinear los programas de seguridad de OT y TI.



Las ventajas del Cyber-PHA

Existen múltiples beneficios potenciales que se obtienen al realizar un Cyber-PHA. El más obvio es garantizar la disponibilidad del sistema eliminando el riesgo cibernético del mismo. Pero un Cyber-PHA también puede beneficiar a las prácticas comerciales más generales de una organización. La aplicación de una metodología de Cyber-PHA documenta los procesos de negocio de una organización y requiere la creación de políticas, procedimientos, normas y controles de seguridad de la información alineados con los objetivos de la organización.

— Articulación bien definida de la estrategia de seguridad de la información basada en los objetivos de la organización y de la unidad de negocio.

— Conocimientos de ingeniería definidos y controles de seguridad alineados basados en el riesgo y los objetivos empresariales.

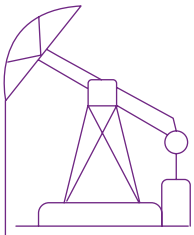
— Dotación de personal eficaz y segura, resultante de las funciones y responsabilidades establecidas.

— Identificación interconectada de las causas e impactos del sistema que facilita la gestión de la vulnerabilidad y el riesgo.

— Respuesta cibernética y gestión de incidentes dirigida y priorizada.

— Métricas, informes y requisitos tecnológicos definidos por SecOps (operaciones de seguridad) para ayudar a cumplir los objetivos empresariales.

Un Cyber-PHA también proporciona a las organizaciones la visibilidad desde el punto de vista cibernético que puede aprovecharse para acelerar la convergencia ICS/OT y TI, ayudando así a lograr lo que se está convirtiendo rápidamente en un objetivo estratégico clave para muchas empresas. La convergencia de ICS/OT y TI tiene el potencial de crear y agilizar el intercambio de datos facilitando las operaciones empresariales. Pero los riesgos cibernéticos están obstaculizando esta convergencia de TI/OT, por lo que llevar a cabo un riguroso Cyber-PHA que ayude a identificar el riesgo operacional, las mitigaciones necesarias y el riesgo residual, puede proporcionar los datos para dar confianza a la gestión en la búsqueda de la agenda de convergencia.



El Cyber-PHA es una **metodología orientada a la seguridad** para identificar y evaluar el riesgo cibernético de los dominios ICS/OT y los sistemas instrumentados de seguridad (SIS).

El Cyber-PHA en el radar regulador

Pero el Cyber-PHA no es sólo una cuestión de beneficios potenciales para las empresas y de buenas prácticas, sino que también está entrando en el radar normativo y puede, en diferentes formas, llegar a ser obligatorio en los próximos años.

De hecho, en Arabia Saudita la Autoridad Cibernética Nacional ya ha puesto en marcha un nuevo marco normativo para la Tecnología Operativa que incluye una revisión específica para que las entidades de petróleo y gas y otras infraestructuras circuitales lleven a cabo un análisis formal de los peligros del proceso que debe incluir, como mínimo, un análisis cualitativo de los riesgos cibernéticos.[7]

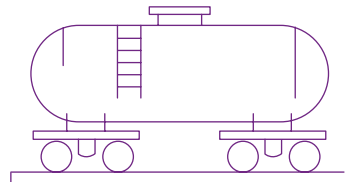
Si se adopta este marco, se convertirá en un requisito reglamentario obligatorio, que podría entrar en vigor a finales de este año.

[7] National Cybersecurity Authority, Operational Technology Cybersecurity Controls (2022)

Mientras tanto, en Estados Unidos, el Departamento de Seguridad Nacional (DHS) ha introducido nuevas medidas a raíz del ciberataque a los gasoductos del año pasado, que interrumpió el flujo de gasolina y gasóleo en la Costa Este. El DHS emitió dos directivas de seguridad de la Administración de Seguridad de Transporte (TSA) que incluyen una serie de medidas que los propietarios y operadores de oleoductos y gasoductos críticos deben aplicar.[8] La primera directiva incluye orientaciones sobre la notificación de incidentes de ciberseguridad, el nombramiento de un coordinador cibernético de la organización y la evaluación de las deficiencias. La segunda directiva es la que tiene más peso, ya que exige medidas específicas de mitigación, un plan formal de contingencia y respuesta en materia de ciberseguridad y una revisión anual de la arquitectura de ciberseguridad.

Estos requisitos, que también incluyen la necesidad de llevar a cabo un análisis del tráfico de red en los sistemas OT, pueden considerarse casi como un "Cyber-PHA-lite". En realidad, lo que el DHS pide a estas empresas es que adquieran pronto una apreciación de los componentes de ciberseguridad y de las comunicaciones de todo el sistema, así como de las interdependencias de TI y OT y de las protecciones que existen o no existen.

Por otra parte, la norma 61511 de la Comisión Electrotécnica Internacional (CEI) sobre seguridad funcional exige ahora una evaluación del riesgo de seguridad del SIS. El informe actualizado resume el procedimiento de evaluación de riesgos denominado Cyber-PHA. El enlace al PHA es un paso en la evaluación de riesgos para, en primer lugar, revisar los resultados de la PHA con el fin de identificar las peores consecuencias para la salud, la seguridad y el medio ambiente (HSSE) del activo y, en segundo lugar, para identificar cualquier escenario de peligro.



El objetivo es establecer **requisitos reglamentarios más formales** en torno a los aspectos de la seguridad operativa relacionados con la ciberseguridad, el mismo ámbito para el que se ha diseñado el Cyber-PHA.

Otro ejemplo procede de la Asociación de Usuarios de Tecnologías de Automatización en las Industrias de Proceso (NAMUR), que ya ha publicado una hoja de trabajo (NA 163) titulada "Evaluación de riesgos de seguridad del SIS". En ella, se puede utilizar una metodología de Cyber-PHA para evaluar los riesgos relacionados con los factores de escalada de ciberseguridad identificados y las mitigaciones recomendadas para reducir los riesgos hasta un determinado nivel. Al crear un puente entre los métodos de PHA y los métodos de evaluación de riesgos de ciberseguridad, los sistemas de seguridad se vuelven más robustos frente a los ataques de ciberseguridad.

En resumen, el objetivo es establecer requisitos reglamentarios más formales en torno a los aspectos de la seguridad operativa relacionados con la ciberseguridad, el mismo ámbito para el que se ha diseñado el Cyber-PHA. En la actualidad, puede haber pocas jurisdicciones que se muevan de forma explícita hacia la regulación del Cyber-PHA, pero el número puede aumentar rápidamente. Además, debido a la naturaleza global e interconectada de la industria de la energía y de los recursos naturales, es probable que los requisitos de una jurisdicción sean percibidos por otras. Por ejemplo, si una gran empresa que opera en Arabia Saudita está obligada a llevar a cabo un ciberproyecto, es posible que pida a las organizaciones con las que trabaja en otras partes del mundo que también lo lleven a cabo. Al final, la marea alta levanta todos los barcos.

[8] Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators (2021)

Cómo puede ayudar KPMG

Las firmas de KPMG ya han ayudado a varios clientes liderando y realizando un Cyber-PHA. Nuestros equipos multidisciplinares, con amplia experiencia en el sector, trabajan estrechamente con los CISO, los CTO y los equipos de Riesgos a nivel corporativo, así como con los Directores de Planta, Operaciones y otros actores clave del dominio ICS/OT.

Por ejemplo, ayudamos a un cliente de la firma que necesitaba estandarizar sus procesos en un entorno heterogéneo de sistemas de múltiples proveedores, llevando todos al mismo nivel de seguridad operativa. Tras una evaluación de las deficiencias y entrevistas con las partes interesadas, realizamos un análisis basado en el Cyber-PHA como parte de la respuesta, junto con otras evaluaciones técnicas de seguridad, el diseño de zonas y conductos para dos tipos diferentes de red ICS, y el diseño de paneles de control para comprender mejor la exposición al riesgo.

Si desea hablar de cualquier aspecto de una ciberevaluación de la seguridad y de cómo se relaciona con su postura de seguridad de TI y OT, no dude en ponerse en contacto con nosotros. Al fin y al cabo, todo parece indicar que los requisitos del Cyber-PHA están llegando y que pronto se esperará que un número cada vez mayor de actores industriales los cumplan.

About the authors

Hossain Alshedoki
IT/OT Cyber Security & Data Privacy Energy and Natural Resources Lead, KPMG in Saudi Arabia
E: halshedoki@kpmg.com

Hossain is an IT/OT Cyber Security leader, specializing in leading teams within a converged business and operational technology environment. Hossain provides intermediary client stakeholder guidance from technical design to board level in areas that utilizes Industrial Controls Systems (ICS), Big Data integration, SCADA, DCS, SIS, IoT and IIoT. Hossain comes from an engineering background with a Cyber Security focus on technical critical infrastructure and consulting in different sectors have been instrumental in the firm's growth and success within the Cyber Security space and a major contributor to the Kingdom of Saudi Arabia vision 2030 on a national level.

Tim Johnson
Director Advisory, Cyber Security Services KPMG in the US
E: timjohnson@kpmg.com

Tim is a seasoned cyber security leader with significant experience leading some of the world's most influential organizations through cyber security transformation of Industrial Control System (ICS) technology and governance. During Tim's career in critical infrastructure and consulting, he has built a reputation for safeguarding ICS availability while implementing cyber security and governance requirements across various industries.

Acknowledgments

This magazine would not be possible without the collaboration from colleagues around the world who generously contributed their support, knowledge and insights into the planning, analysis, writing and production of this report. Thank you to Tzouliano Chotza, Lyndie Dragomir, Nicole Duke, Mark Hamilton, Carmen Millet and Richard Turitz.

Contacts

Regina Mayor
Global Head of Energy
KPMG International
E: rmayor@kpmg.com

Valerie Besson
Regional Energy & Natural Resources Leader for Europe/Middle East/Africa (EMA) and National Sector Leader, Energy and Utilities
KPMG in France
E: valeriebesson@kpmg.fr

Manuel Fernandes
Regional Energy & Natural Resources Co-Leader for Americas and National Oil & Gas Leader
KPMG in Brazil
E: mfernandes@kpmg.com.br

Ronald Heil
Global Cyber Security Leader for Energy and Natural Resources
KPMG in the Netherlands
E: heil.ronald@kpmg.nl

Angela Gildea
Regional Energy & Natural Resources Co-Leader for Americas and National Sector Leader, Energy, Natural Resources and Chemicals
KPMG in the US
E: angelagildea@kpmg.com

Jonathon Peacock
Regional Energy & Natural Resources Leader for Asia Pacific (ASPAC) and Oil & Gas Leader
KPMG Australia
E: jjpeacock@kpmg.com.au

home.kpmg/drillingdown

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name:Drillng Down
Publication number: 138002-G
Publication date: April 2022