Deloitte. | aws

Securing CPS Environments with the Cybersecurity Atlas Model for Modern Utilities

January, 2026

01

Navigating the Fragmented Landscape of Cyber-Physical Security

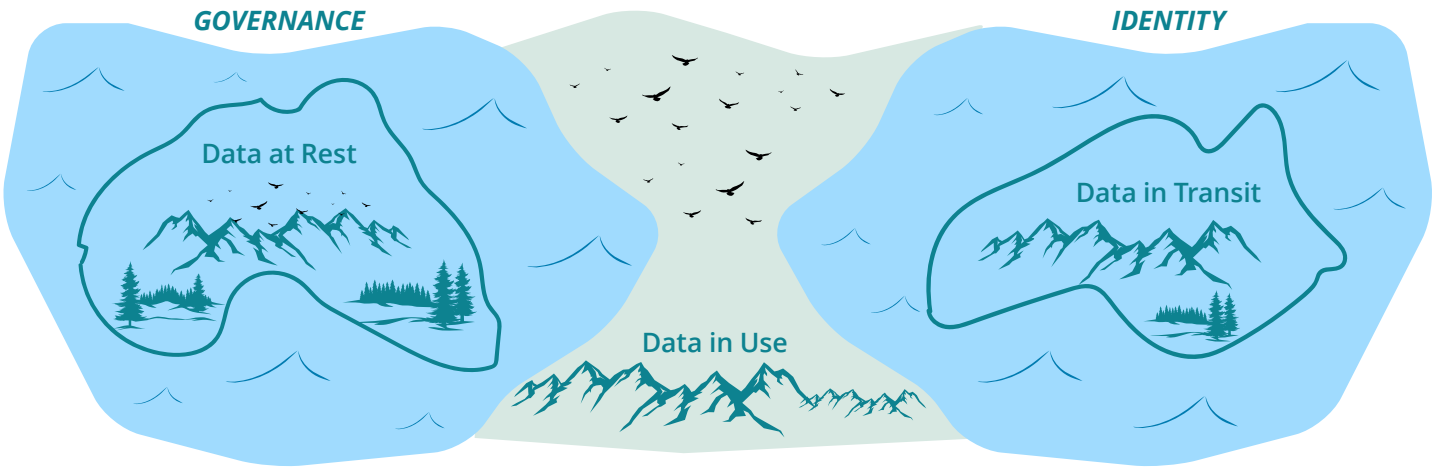
The convergence of operational technology (OT) and information technology (IT) in utility environments has created unprecedented cybersecurity challenges. With critical infrastructure increasingly connected and digitalized, organizations face the complex task of securing both legacy systems and modern technologies.

In the wake of a recent cybersecurity incident, a utility organization swiftly deployed a suite of new security tools to remediate vulnerabilities. Yet, despite their intentions, these solutions failed to integrate effectively with the existing technology stack. The result was a fragmented environment, security controls operating in isolation, critical data flows disrupted, and operational resilience compromised. This scenario is too common in cyber-physical systems (CPS), where security is often layered atop legacy infrastructure as an afterthought rather than embedded by design.

Historically, utility environments were engineered for reliability and stability, and less of a focus on security. Devices were deployed to perform specific functions, with communications and integrations evolving incrementally over time. When cybersecurity measures were eventually introduced, they frequently arrived in response to audits, regulatory requirements, or incidents. The outcome is a patchwork of protections: encryption securing smart meters, segmentation at substations, multi-factor authentication at operator consoles. Each measure addresses a discrete risk, but rarely do they coalesce into a unified, end-to-end defense strategy.

This whitepaper introduces the Cybersecurity Atlas Model: a approach to CPS security that begins with understanding how data moves, where it resides, and when it is processed. The Cybersecurity Atlas Model empowers operators to visualize their environment as an interconnected landscape and better understand the terrain they're working with.

Figure 1 – Cybersecurity Atlas Model

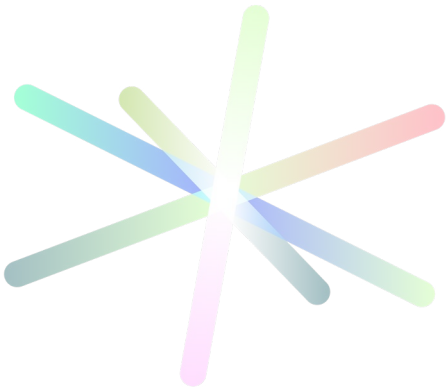


The Cybersecurity Atlas Model organizes data into three fundamental "continents" each representing a critical domain for security controls: at rest, in transit, and in use. Crucially, the Cybersecurity Atlas Model also introduces a fourth feature, "Oceans" that engulf the environment: governance and identity. This feature determines that policy enforcement, user accountability, and operational visibility are consistently applied, providing the context and traceability required for effective risk management.

By shifting the focus from isolated tools and compliance checklists to the operational realities of CPS environments, the Cybersecurity Atlas Model fosters a shared understanding among IT, OT, and engineering teams. It enables organizations to prioritize protections based on risk (based on factors such as likelihood, impact, criticality, and timing), regardless of whether the environment comprises a million smart meters or a handful of Programmable Logic Controllers (PLC).

As organizations accelerate adoption of cloud platforms, distributed energy resources, and Artificial intelligence (AI) and machine learning (ML) driven automation, the traditional boundaries between IT and OT are dissolving. New systems are layered onto legacy infrastructure, increasing complexity and risk. The Cybersecurity Atlas Model offers a pragmatic way to align security investments with the realities of modern utility operations, providing not another framework, but a map to guide purposeful action.

This paper further demonstrates how Amazon Web Service (AWS)'s suite of cloud-native services, combined with Deloitte's deep experience in CPS security implementation and integration, aligns with the Cybersecurity Atlas Model. Also included within this paper are mappings of AWS and Deloitte capabilities, illustrating how integrated solutions can be applied to utility systems at scale. Ultimately, the message is clear: effective cybersecurity is not about just adding more tools or frameworks, but about gaining the visibility and understanding needed to secure what matters.



02

Why Data, Not Just Physical Assets, Should consider Be the Focus of Cyber-Physical Security

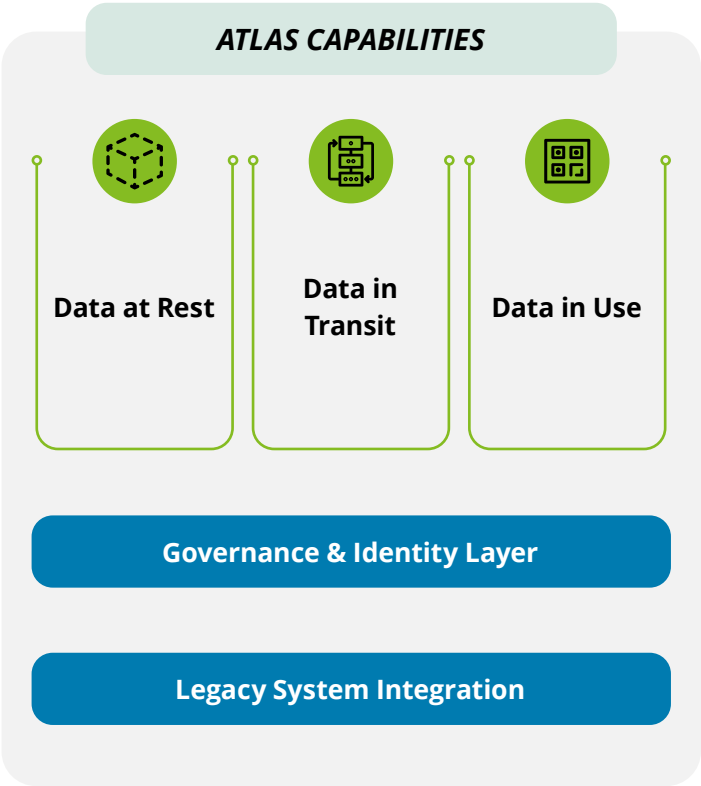
Traditional approaches to cybersecurity in CPS have long centered on the protection of physical assets. Devices such as smart meters, remote terminal units (RTUs), PLCs, and relays are the visible endpoints that underpin utility operations. As a result, security strategies often begin and end with safeguarding these devices. However, in practice, the true target for adversaries is not the device itself, it is the data that powers the system.

Each operational process within a utility environment is fundamentally driven by data. Voltage readings, outage notifications, pricing signals, and breaker commands lean on the timely and careful flow of information. Securing the physical device, while required, is insufficient if the data it generates, transmits, or processes remains vulnerable. The availability, integrity, and confidentiality of this data are what ultimately sustain operational resilience.

Recognizing this, the Cybersecurity Atlas Model reframes cybersecurity around the three core states of data:

- Data at rest: Information stored in memory, logs, databases, or on devices.
- Data in transit: Data moving across networks or field communication links.
- Data in use: Information actively processed, displayed, or acted upon by applications or human operators.

Figure 2 – Atlas Capabilities in Cybersecurity



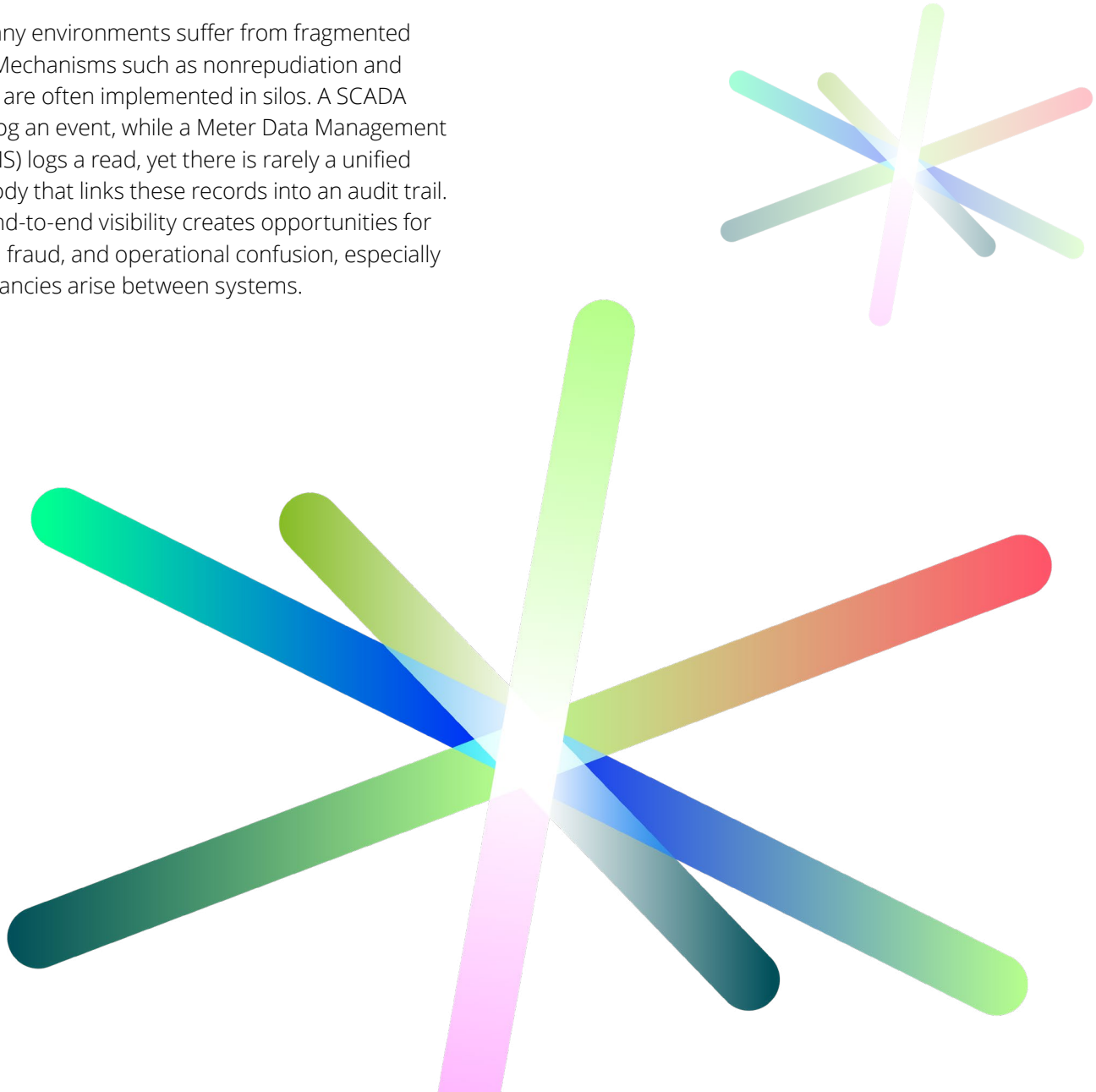
Each state introduces distinct risks and attack surfaces. For example, securing a meter's memory is ineffective if it's network uplink is exposed, allowing adversaries to inject spoofed readings. Encrypting Supervisory Control and Data Acquisition (SCADA) traffic is only part of the solution; if the human-machine interface (HMI) is left unprotected, attackers can manipulate what operators see and do, undermining system trust.

In dynamic operational environments, teams often default to protecting the many visible elements, typically the device itself or its immediate network segment. While this approach addresses tactical concerns, it overlooks the broader, strategic imperative: safeguarding the data lifecycle. Operational integrity depends not just on isolated controls, but on a broad view of how data moves, where it resides, and how it is used.

Moreover, many environments suffer from fragmented protections. Mechanisms such as nonrepudiation and event logging are often implemented in silos. A SCADA system may log an event, while a Meter Data Management System (MDMS) logs a read, yet there is rarely a unified chain of custody that links these records into an audit trail. This lack of end-to-end visibility creates opportunities for manipulation, fraud, and operational confusion, especially when discrepancies arise between systems.

The Cybersecurity Atlas Model addresses these challenges by organizing security controls around the actual behavior and lifecycle of data, rather than its physical location. By mapping how data flows through the environment, organizations can apply the appropriate controls, at the applicable point, at the applicable time, to enable both security and operational continuity.

Ultimately, this data-centric approach transforms security from a reactive defense mechanism into an integral part of the system's architecture. When protections are aligned with the flow and use of data, cybersecurity becomes a driver of reliability, trust, and business value.



03

Building a Common Operating Picture Across Teams

In complex CPS environments, cybersecurity challenges rarely stem from a lack of technical experience. Instead, they often arise because teams operate from different vantage points, each with its own priorities, tools, and language. IT teams manage identity, credentials, and network infrastructure; OT teams oversee field devices and SCADA communications; engineering teams focus on performance, control logic, and reliability. When incidents span multiple domains—such as telemetry delays, certificate failures, or malformed commands—no single group holds the full operational picture.

The Cybersecurity Atlas Model addresses this gap by providing a unified map of the system's data lifecycle and its supporting governance "oceans" and "continents". Rather than imposing a rigid framework, the Cybersecurity Atlas Model enables each team to visualize how data moves through the environment and where their responsibilities intersect with those of others.

Just like in a real Atlas we can consider that the three data states are the "continents" of the Cybersecurity Atlas (at rest, in transit, and in use). Governance and identity form the "oceans" between them. This is the link between the "continents" and enable policies, credentials, and audit trails to flow effectively across the organization. These cross-cutting elements are not confined to a single data state; instead, they underpin the system, enabling continuity and trust.

This approach surfaces the interdependencies that can otherwise remain hidden. Like in the real world, what happens on one "continent" often affects what reaches another. For example, a broken trust policy in the "ocean" of identity can compromise data in each state, regardless of how well individual devices or network segments are protected. By clarifying where each team's visibility and responsibility begin and end, the Cybersecurity Atlas Model encourages collaboration and reduces the risk of gaps or overlaps in coverage.

The Cybersecurity Atlas Model does not merge or dilute team responsibilities. Instead, it bridges them, enabling IT, OT, and engineering to consult the same map, ask different questions, and coordinate their actions more effectively. Whether the focus is on securing edge devices, managing credentials, or tuning control algorithms, the Cybersecurity Atlas Model provides a shared reference point.

Just as navigational maps are tailored to their specific purpose (maritime charts for depth and currents, airspace maps for altitude and control zones) the Cybersecurity Atlas Model can be adapted to the mission of each CPS environment. A smart metering deployment may emphasize identity management and cloud integration, while a transmission operator may prioritize deterministic data flows and device integrity. The underlying structure remains consistent, but its application is flexible.

Ultimately, the value of the Cybersecurity Atlas Model lies in its ability to foster a common operating model. By aligning teams around a shared understanding of the system, it can empower organizations to respond to incidents, manage risk, and drive operational excellence, no matter how diverse their roles or objectives may be.

04

What an Atlas Really Provides

The Cybersecurity Atlas Model serves to visualize the complexity of cyber physical security data and the interconnected operational environments. The Cybersecurity Atlas Model grounds cybersecurity in something universally familiar. Much like a geographic atlas assembles individual maps into a coherent picture of the world, the Cybersecurity Atlas Model unites disparate tools used in cybersecurity to protect data into a single, navigable landscape.

The Cybersecurity Atlas Model is not intended to replace established industry frameworks such as the Purdue Model or IEC 62443. Nor is it a prescriptive blueprint that dictates many control, protocol, or technology an organization should consider deploying, just as a world atlas does not show many the details of a continent.

This approach allows stakeholders to see beyond the individual functions of each cybersecurity tool, revealing how the data interacts, overlaps, or leaves gaps in the overall defense posture. The Cybersecurity Atlas Model leverages the well known cybersecurity principle of protecting data at rest, in transit, and in use, mapping each tool's role in safeguarding data throughout its lifecycle. By aligning security tools to these data states, operators gain a clearer view of where protections are strong, where redundancies exist, and where vulnerabilities may persist.

By mapping tool coverage against operational processes and data flows, the Cybersecurity Atlas Model clarifies both operational dependencies and potential security vulnerabilities. It highlights the critical pathways where multiple protections can reinforce each other or where a single point of failure could have cascading effects across operations.

By grounding the concept in something universally familiar, the Cybersecurity Atlas Model helps transform cybersecurity from a fragmented collection of point solutions into an integrated, strategic capability. It becomes easier to communicate potential risks, spot redundancies, and coordinate improvements across engineering, operations, and security teams. The result can be a clearer path to building a unified, resilient defense posture one that evolves alongside the operational environment.

05

Mapping Tools to the Cybersecurity Atlas Model

Many utility environments already have cybersecurity tools in place. But those tools are usually deployed based on network zones, compliance requirements, or vendor recommendations, and not based on how data moves through the system.

The Cybersecurity Atlas Model takes a different approach. It aligns protection tools to where data exists in the lifecycle (at rest, in transit, and in use) and identifies the "states" within each where those tools provide an increased benefit. It also makes room for governance and identity. The elements that span each data state and bind the system together.

This section provides a mapping of common AWS security tools to each part of the Cybersecurity Atlas Model. It is not a checklist, it is a guide for evaluating whether the applicable controls are deployed where the data circumstances protection.

Continent: Data at Rest

State	*What's at Risk*	*Tools That Apply (AWS)*
Meter Memory	Stored usage logs, configuration data	Encrypted flash storage, secure firmware, anti-tamper protection (AWS IoT Greengrass)
Collector Buffers	Unprocessed field data queued for uplink	Access control on local operating systems (OS), data deletion policies (AWS IoT Greengrass – Stream manager)
Substation Logs & Configs	Fault records, logic files, relay settings	File integrity monitoring, secure boot, segmented storage (AWS IoT Greengrass – Log Manager, Shadow Manager)
Meter Data Management System (MDMS) & Historians	Long-term billing and event data	Role based access control (RBAC) in apps, audit trails, data encryption at rest, backup integrity validation (Amazon S3, Amazon Key Management Service (KMS))

Continent: Data in Transit

State	What's at Risk	Tools That Apply (AWS)
Field to Collector	Radio Frequency (RF) mesh spoofing, injection attacks	Mutual TLS, replay protection, device certificates (AWS IoT X.509 Certificates, Custom CAs)
Collector to Head-End	VPN hijack, command injection	IPSec tunnels, private Access Point Names (APNs), SIEM-integrated alerting (AWS IoT Defender, AWS IoT VPN, AWS Network Firewall)
Substation to SCADA	Latency-sensitive telemetry, Distributed Network Protocol 3 (DNP3) fuzzing	Protocol-aware firewalls, encryption with deterministic transport (AWS Network Firewall, AWS Direct Connect)
Enterprise to Control Systems	IT/OT bridge traffic	One-way gateways (data diodes), required identity-based routing (AWS Network Firewall, AWS IAM, AWS PrivateLink)
Cloud Integrations	Distributed Energy Resource Management Systems (DERMS), outage response, DR partners	Federated IAM, encrypted APIs, external policy enforcement (AWS IAM, AWS API Gateway)

Continent: Data at in Use

State	What's at Risk	Tools That Apply (AWS)
SCADA/HMI Operations	Operator impersonation, command spoofing	Multi-Factor Authentication (MFA), role-based views, keystroke and action logging (AWS IAM, Amazon CloudWatch)
Embedded Logic	Corrupted firmware, modified control decisions	Control logic hashing, secure firmware validation, memory protection (AWS IoT Device Defender, AWS KMS)
Analytics Platforms	Poisoned data, model drift	Input validation, model integrity checks, audit trails (Amazon SageMaker, AWS CloudTrail)
Automated Responses	Breaker trips, AMI shutoffs, DER changes	Real-time alerts, escalation policies, command origin tracing (Amazon EventBridge, AWS Security Hub)

Meta Layer: Governance and Identity ("The Oceans")

State	*What's at Risk*	*Tools That Apply (AWS)*
User Identity	Access misuse, credential reuse	Identity federation, centralized IAM, least privilege enforcement (AWS IAM, AWS IAM Identify Center)
Device Identity	Spoofed endpoints	X.509 certs, secure onboarding, hardware root of trust (AWS Certificate Manager, AWS IoT Core)
Audit & Traceability	Lack of non-repudiation	Immutable logs, hash chains, blockchain-inspired audit trails (AWS CloudTrail, Amazon Managed Blockchain)
Policy Enforcement	Inconsistent configurations	Configuration baselines, security-as-code, policy assertion (AWS Config, AWS CloudFormation, AWS CDK)
Data Classification	Overexposed sensitive data	Sensitivity tagging, dynamic access controls (AWS Macie, AWS IAM, AWS RAM)

06

Deloitte, capabilities (the cartographer) of the Cyber Security Atlas Model

Many utilities already have some controls in place, firewalls at substations, encrypted databases, and endpoint protection on operator workstations. The problem isn't tool shortage. The problem is alignment.

Alignment between teams. Alignment between tools and threats. Alignment between what's documented and what's running in the field.

Deloitte helps organization address this by taking a system-level view of cybersecurity. Their work isn't limited to assessment or point-in-time compliance. It's built around helping CPS operators govern, build, and monitor systems that are secure by design, and stay that way as they scale or modernize.

But alignment only becomes possible when you can see the many landscape, not just one domain or tool at a time, but how they fit together. That's where the Cybersecurity Atlas Model comes in.

Picture yourself describing Earth to someone who hasn't seen it. Naturally, you'd start with what you know: your neighborhood, city, or country. You might paint a vivid, careful picture of your region, but inevitably miss many continents, vast oceans, and diverse landscapes that full our planet's story. Your description may likely be precise yet incomplete.

Cybersecurity often faces the same challenge. Each professional within an organization brings deep, specialized knowledge of their domain, whether network architecture, operations, application security, or regulatory compliance. Yet, because each individual views the cybersecurity or operational landscape through their own specialized lens, it's difficult to integrate those viewpoints into a unified understanding.

Just as a geographic atlas solves this problem by combining individual maps into a view of the world, Deloitte acts as the cartographer of cybersecurity. Using the Cybersecurity Atlas Model, Deloitte integrates tools, frameworks, and concepts into a single, coherent landscape. The Cybersecurity Atlas Model provides a way to understand the complexity of cyber-physical systems and interconnected operational environments, without losing sight of the bigger picture.

By establishing this common reference point, Deloitte helps enable organizations to:

01
Align their experience across different domains and specializations

02
Identify blind spots that might otherwise go unnoticed in siloed approaches

03
Visualize connections between their specialized contributions and the broader security ecosystem

04
Coordinate efforts to protect data at rest, in transit, and in use

The Cybersecurity Atlas Model doesn't diminish the importance of specialized knowledge; instead, Deloitte provides the connective tissue that can transform individual experience into collective security strength—just as a cartographer transforms scattered observations into a map you can trust.

Deloitte Services Mapped to the Cybersecurity Atlas Model

Atlas Element	*Deloitte Capabilities*
Data at Rest	Secure firmware lifecycle management, encrypted storage integration, tamper-proof logging, data governance design
Data in Transit	Protocol hardening (DNP3, Modbus, IEC 61850), secure mesh/LTE architecture, identity-based routing, VPN and private link design
Data in Use	Runtime application protection, control logic substantiation, operator access hardening, HMI and SCADA security design
Governance & Identity Layer	CPS security program development, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) and International Organization for Standardization (ISO) 27001 readiness and remediation, policy enforcement strategy, identity and access management (IAM) implementation
Legacy System Integration	Risk assessments secure segmentation strategy, asset lifecycle alignment with modern toolsets

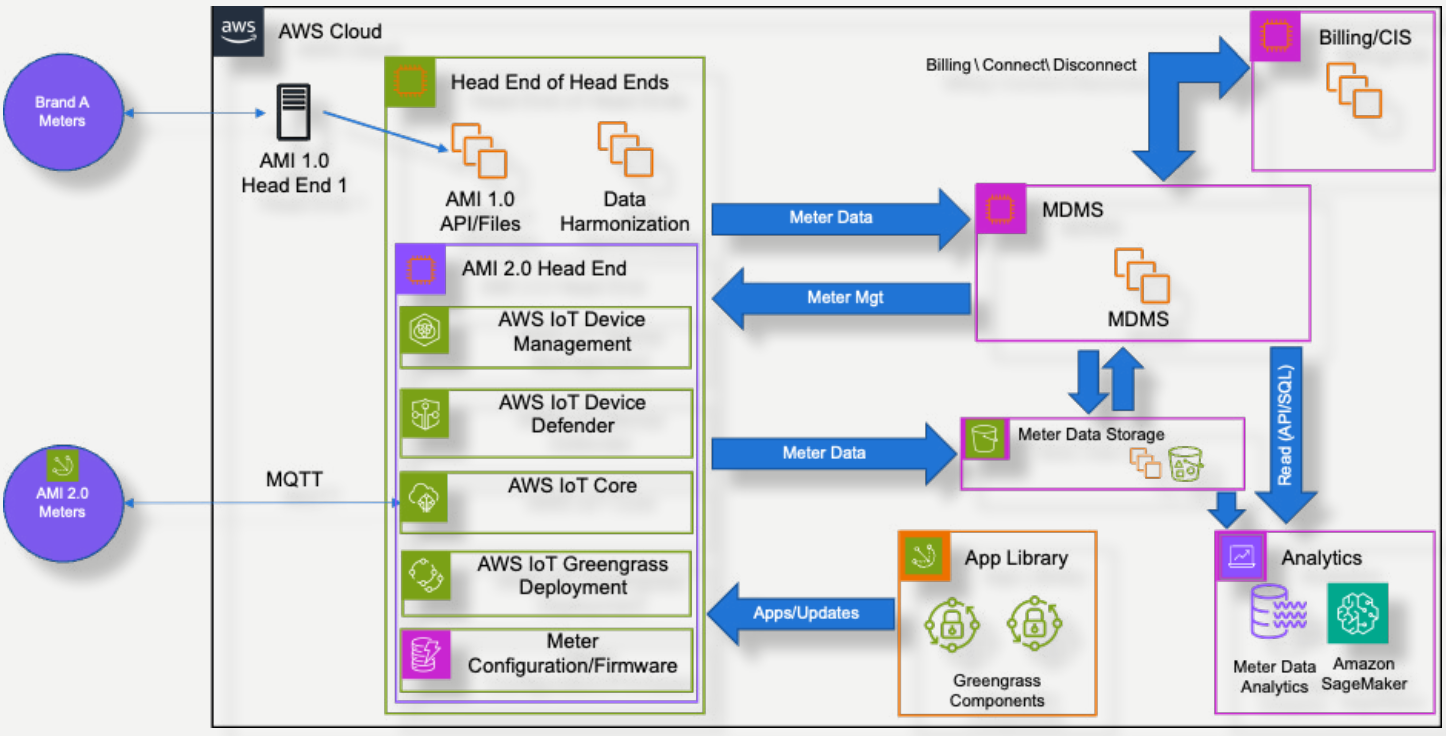
07

Applying the Cybersecurity Atlas Model: Smart Metering

This section demonstrates how the Cybersecurity Atlas Model materializes in an implementation through a smart metering infrastructure using AWS services. Rather than presenting an abstract architecture, this example illustrates how a data-centric security approach transforms theoretical concepts into practical solutions.

Smart metering represents an high-quality case study for the Cybersecurity Atlas Model, as it encompasses the three fundamental data states while highlighting the critical importance of the governance layer. The implementation begins with data at rest, where meter readings and configuration data should consider be protected both in the cloud and at the edge. Amazon Simple Storage Service (S3) provides the primary storage backbone, employing AWS KMS encryption to secure accumulated meter data, while AWS IoT Greengrass enables secure local storage at the meter level for maintaining operations during communication interruptions.

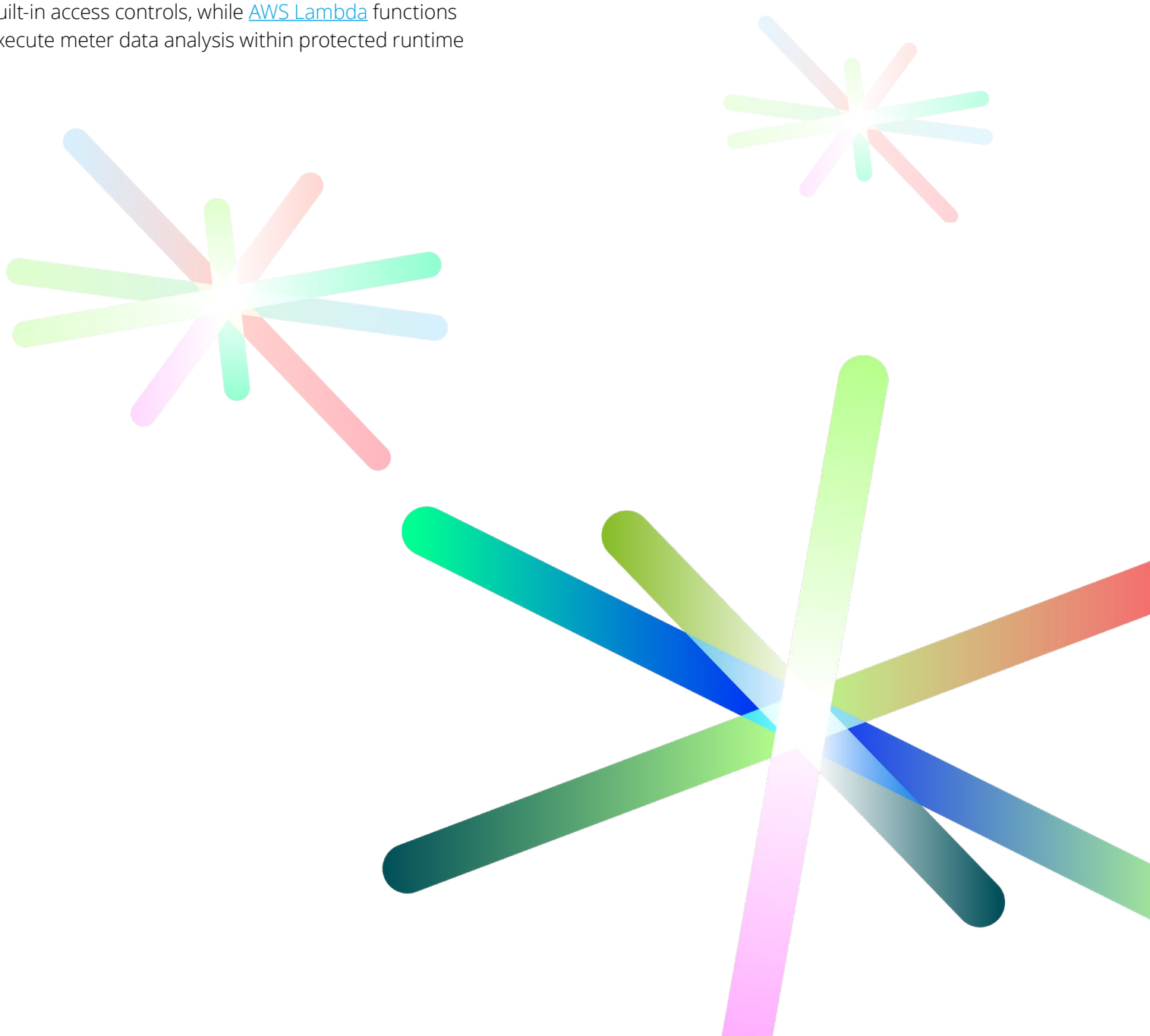
Figure 3 – AWS Cloud data in transit model layers



The data in transit layer presents different challenges in smart metering environments, where information should consider flow securely across multiple networks and protocols. AWS IoT Core serves as the cornerstone for meter-to-cloud communication, implementing TLS 1.2 encryption and certificate-based authentication. For existing Advanced Metering Infrastructure (AMI) head-end systems, Amazon API Gateway provides secure integration points with mutual authentication, while AWS PrivateLink enables service-to-service communication to remain protected within the AWS network boundary.

When it comes to data in use, smart metering systems require real-time processing capabilities while maintaining security. AWS IoT enables secure data processing with built-in access controls, while AWS Lambda functions execute meter data analysis within protected runtime environments. This processing layer is particularly critical for use cases like demand response, where decisions should be made efficiently while maintaining data integrity.

This implementation demonstrates how the Cybersecurity Atlas Model's principles translate into concrete architectural decisions. By organizing security controls around data states rather than traditional network boundaries, utilities can better protect their smart metering infrastructure while maintaining operational efficiency. The potential result is a system that not only secures individual components but determines end-to-end protection of meter data throughout its lifecycle.



08 AWS Cyber Security Services

AWS helps organizations to develop and evolve security, identity, and compliance into specific business enablers. Security is AWS' top priority, while AWS offers over 300 cloud security tools, this section focuses on specific services that directly aid the Cybersecurity Atlas Model's implementation in utility environments, particularly for smart metering and grid operations.

Figure 4 – AWS Security, Identity, and Compliance Solutions

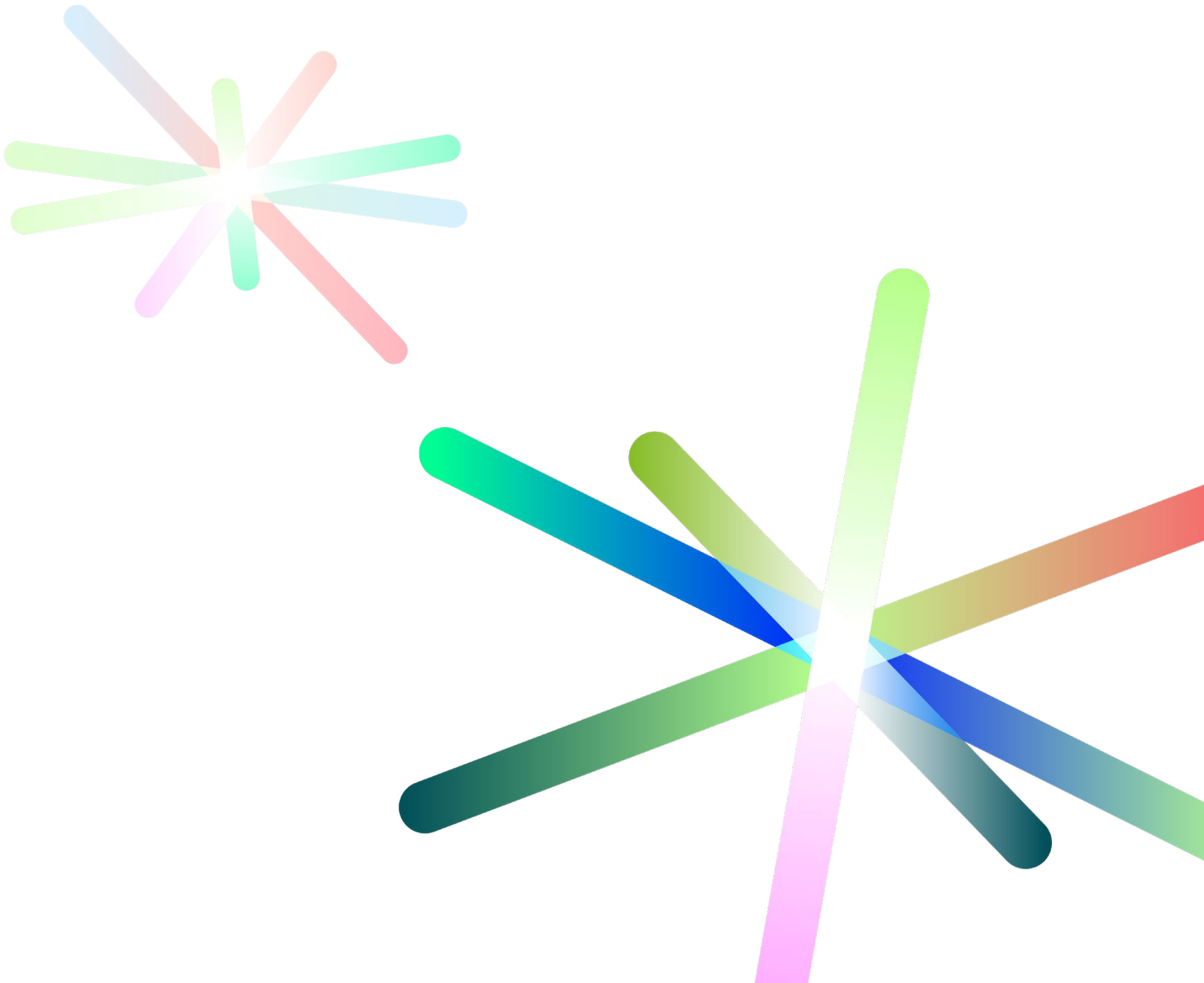
AWS IAM forms the foundation of the identity layer, providing granular control over who can access what resources and under what conditions. In smart metering deployments, IAM enables utilities to define precise roles for different operational functions.

The protection of data at rest depends heavily on **AWS KMS**. In utility environments, where data sensitivity varies from routine meter readings to critical grid control commands, AWS KMS enables different encryption schemes for different data classifications.

For real-time security monitoring, Amazon GuardDuty provides continuous threat detection across the utility's AWS infrastructure. By analyzing AWS CloudTrail logs, VPC flow logs, and DNS logs, Amazon GuardDuty can identify potential security issues such as unauthorized access attempts to meter data or unusual API calls.

AWS Security Hub serves as the central dashboard for security operations, aggregating findings from multiple AWS security services and providing a detailed view of the utility's security posture.

The integration of these services creates a cohesive security framework that aligns with the Cybersecurity Atlas Model's emphasis on data-centric protection. Rather than treating security as a collection of objective tools, this approach can enable protections to work together across the data states - at rest, in transit, and in use - while maintaining consistent governance and visibility.



09

Why This Matters in CPS Environments

CPS, especially in critical infrastructure, don't run on clean-slate architectures. They run on vendor-constrained equipment, 20-year-old firmware, and networks that were not meant to talk to the cloud. This is where Deloitte's cross-domain experience provides its value.

01

Industrial environments: Experience securing substations, pipelines, smart buildings, and grid operations

02

Product security: Assisting manufacturers of AMI devices, RTUs, and smart meters in embedding security at the hardware and firmware level.

03

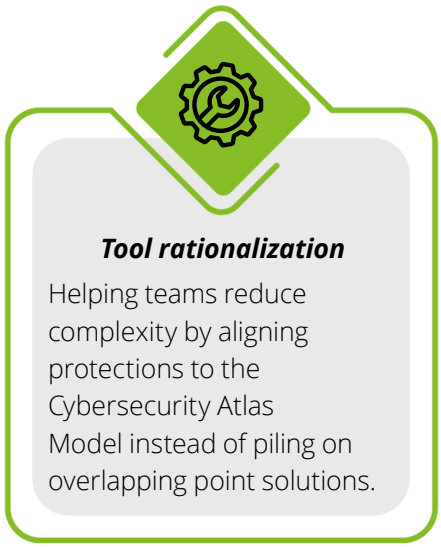
Multi-sector insight: Applying practices demonstrated in automotive, medical, oil/gas, chemicals, aerospace, and other critical infrastructure industries to utility environments with adaptation, not copy-paste.

10

What Deloitte Brings to the Table

Real world readiness:

Assessments and remediation plans that reflect how the systems run, not just how they should run.



Tool rationalization

Helping teams reduce complexity by aligning protections to the Cybersecurity Atlas Model instead of piling on overlapping point solutions.

Program visibility

Mapping the organization's tools, controls, and risks across the data lifecycle in ways that can be used by engineering, IT, cybersecurity, and executive leadership.

The Cybersecurity Atlas Model doesn't replace Deloitte's services. It clarifies where those services land. Whether it's hardening embedded logic at the edge, securing transit over a public network, or helping coordinate responses to an audit finding. The Cybersecurity Atlas Model provides a shared map to work from. Deloitte helps translate that map into action.

11

Applying the Cybersecurity Atlas Model to Smart Meters, EV Chargers, and Distributed Devices

The Cybersecurity Atlas Model view isn't just conceptual; it's made to work with real systems. Utilities today are deploying or managing millions of distributed endpoints: AMI meters, EV chargers, sensors, DERs, and public infrastructure. These aren't protected by a central firewall or inside a facility. They sit in parking lots, on poles, in garages, and behind customers' homes.

Each one generates data. Each one communicates. And each one introduces a surface where security has to work without adding friction.

The Cybersecurity Atlas Model helps break these systems down by function, not vendor or architecture. Below we have another example of how the Cybersecurity Atlas Model's view maps to a common CPS deployments: EV charging networks.

EV Charging Infrastructure

Atlas Layer	*Example in EV Charging*	*What You Secure*
Data at Rest	Charger local logs, rate plans, firmware settings	Secure configuration storage, audit logging, OTA update protection (AWS KMS, AWS IOT Core)
Data in Transit	Vehicle-to-charger handshake, charger-to-cloud	Authenticated API traffic, certificate-based communications, protocol validation (AWS Certificate Manager, Amazon API Gateway)
Data in Use	Load balancing systems, billing logic, fleet dashboards	HMI authentication, load shedding logic integrity, session billing validation (AWS IAM, Amazon EventBridge)
Governance & Identity Layer	User identity, charge session proof, policy enforcement	Role-based access to dashboards, usage logging, integration trust boundaries (AWS Organizations, AWS CloudTrail, AWS CloudWatch)

Challenge: EV chargers often straddle both the customer domain (personal vehicles, mobile apps) and grid operations (demand response, load shaping). The Cybersecurity Atlas Model allows both sides to see the same flow, without blurring responsibilities.

12

What the Cybersecurity Atlas Model's view helps uncover

The true value of the Cybersecurity Atlas Model emerges when examining real-world utility deployments, where it reveals critical security interconnections that might otherwise go unnoticed. Traditional security approaches, focused on network segments or device types, often miss the subtle ways that data vulnerabilities can cascade through a system.

As we have discussed above, consider a typical smart metering deployment: Strong device-level security becomes meaningless if the data collection path isn't equally protected. Adversaries don't need to compromise the meter if they can inject false readings during transmission or manipulate data as it's processed in the head-end system. Similarly, in EV charging networks, a station might employ broad encryption for payment processing, but if its load management logic can be overridden through an unsecured maintenance interface, both customer privacy and grid stability are at risk.

The power of this approach lies in its ability to align security controls with actual operational processes rather than theoretical network architectures. Through this lens, security becomes less about deploying point solutions and more about understanding and protecting the many data lifecycle. The Cybersecurity Atlas Model serves as both a diagnostic tool and a roadmap, helping organizations uncover hidden vulnerabilities while providing a framework for implementing comprehensive, data-centric security that evolves alongside their CPS landscape.

13

Where AWS and Deloitte Fit

The combination of AWS's cloud infrastructure and Deloitte's implementation experience creates a powerful alliance for utilities implementing the Cybersecurity Atlas Model. AWS provides the foundational security services and scalable infrastructure required for modern utility operations, while Deloitte brings deep industry knowledge and practical experience in navigating the complex landscape of utility cybersecurity.

AWS delivers the technical backbone through services that align with each layer of the Cybersecurity Atlas Model - from IoT device security to data encryption, identity management, and comprehensive monitoring. These services are designed to scale effectively, whether managing thousands of smart meters or millions of real-time sensor readings from across the grid.

Deloitte complements this technical foundation by helping utilities translate the Cybersecurity Atlas Model into practical implementation strategies. Their experience spans critical areas such as compliance mapping for NERC CIP requirements, integration of legacy systems with modern security controls, and development of governance frameworks that align with utility operations. Deloitte's industry experience supports security implementations not only protect assets but also operational efficiency and regulatory compliance.

Together, this relationship enables utilities to implement security solutions that protect data throughout its lifecycle while maintaining the reliability and performance demands of critical infrastructure operations.

14

Oceans and Continents Not Explored within this Whitepaper

The combination of AWS's cloud infrastructure and Deloitte's implementation experience creates a powerful alliance for utilities implementing the Cybersecurity Atlas Model. AWS provides the foundational security services and scalable infrastructure required for modern utility operations, while Deloitte brings deep industry knowledge and practical experience in navigating the complex landscape of utility cybersecurity.

AWS delivers the technical backbone through services that align with each layer of the Cybersecurity Atlas Model - from IoT device security to data encryption, identity management, and comprehensive monitoring. These services are designed to scale effectively, whether managing thousands of smart meters or millions of real-time sensor readings from across the grid.

Deloitte complements this technical foundation by helping utilities translate the Cybersecurity Atlas Model into practical implementation strategies. Their experience spans critical areas such as compliance mapping for NERC CIP requirements, integration of legacy systems with modern security controls, and development of governance frameworks that align with utility operations. Deloitte's industry experience supports security implementations not only protect assets but also operational efficiency and regulatory compliance.

Together, this relationship enables utilities to implement security solutions that protect data throughout its lifecycle while maintaining the reliability and performance demands of critical infrastructure operations.

01 *Cybersecurity Atlas Model & Generative AI (GenAI)*

The emergence of agentic AI, GenAI, and physical AI represents a transformative frontier in smart grid security and operations.

Agentic AI systems, capable of autonomous decision-making, could revolutionize grid management by independently responding to security threats and enhancing power distribution in real time. Yet, this autonomy introduces new security concerns: these AI agents should consider be protected against manipulation while maintaining operational transparency.

GenAI is already reshaping threat detection and response in utility networks by creating dynamic security models that adapt to evolving attack patterns.

Physical AI systems, which integrate computational and physical capabilities, are giving rise to "intelligent" grid components. These can not only detect and respond to threats but also physically reconfigure themselves to maintain stability and security.

This convergence creates a new security paradigm where the boundaries between digital and physical security blur. To remain relevant, the Cybersecurity Atlas Model should consider evolve to encompass AI-driven security orchestration while maintaining robustness across both domains.

02 *Aligning Cyber-Physical Systems with Critical Priorities*

The Cybersecurity Atlas Model provides a distinct lens for aligning protections across safety-critical, mission-critical, and business-critical functions within cyber-physical systems. These categories represent different but interconnected priorities, each requiring tailored resilience strategies.

- **Safety-Critical Systems**

These involve processes where failures could endanger human lives or the environment—such as grid stability, industrial controls, or medical devices. The Cybersecurity Atlas Model helps map how security tools protect data flows that underpin safe operations, supporting vulnerabilities are addressed before they escalate into safety hazards.

- **Mission-Critical Systems**

These suggest the core functions that should consider remain operational at many times - such as grid dispatching, emergency response coordination, or defense systems. By visualizing interdependencies, the Cybersecurity Atlas Model identifies single points of failure and redundancies, enabling organizations to strengthen continuity of operations in the face of evolving cyber threats.

- **Business-Critical Systems**

These enable financial health, service delivery, and organizational reputation. The Cybersecurity Atlas Model clarifies how business-critical data (customer information, billing, market operations) intersects with operational systems, helping leaders balance risk mitigation with performance and compliance requirements.

By situating these priorities within a single navigable model, the Cybersecurity Atlas Model reveals where safety, mission, and business imperatives overlap and where gaps could undermine resilience. This integrated perspective determines cybersecurity is not managed in isolation but as a strategic enabler of safe, reliable, and sustainable operations.

While the Cybersecurity Atlas Model provides a guide for aligning safety-critical, mission-critical, and business-critical priorities as well as the emerging role of GenAI to an organization, each of these domains (continent/ocean) carries complexities that go beyond the scope of this paper. Their interplay with cybersecurity strategy is significant enough to intend deeper exploration, which will be addressed in future whitepapers.

15 *Conclusion*

As utilities continue to digitalize their operations and expand their connected infrastructure, the need for a coherent, data-centric security approach becomes increasingly critical. The Cybersecurity Atlas Model presented in this paper offers more than just another framework - it provides a practical way to visualize, understand, and protect the complex flow of data that powers modern utility operations.

The Model's strength lies in its simplicity: by focusing on the fundamental states of data - at rest, in transit, and in use - along with a cross-cutting governance layer, it creates a common language that bridges the traditional gaps between IT, OT, and engineering teams. This unified view enables utilities to move beyond siloed security approaches and implement protections that align with how their systems actually operate.

Whether securing millions of smart meters, managing distributed energy resources, or protecting critical control systems, the Cybersecurity Atlas Model scales to meet the challenge. It accommodates both legacy infrastructure and emerging technologies, helping utilities build security programs that are both comprehensive and adaptable.

The Cybersecurity Atlas Model transforms cybersecurity from a compliance exercise into a strategic capability. By providing a clear map of how data flows through utility systems, it enables organizations to make informed decisions about security investments, identify critical vulnerabilities, and build resilience into their operations from the ground up.

If you want to know more, you can visit this page, contact us at through our website, or contact one of the authors listed below.

Authors

Jason Hunt
Principal, Cyber Risk | IoT Security Leader
Deloitte & Touche LLP
jashunt@deloitte.com

Akhilesh Bhangepatil
Senior Manager, Cyber Risk | IoT Security Leader
Deloitte & Touche LLP
abhangepatil@deloitte.com

Juan Hernandez
Specialist Master, Cyber Risk | IoT Security Architect
Deloitte & Touche LLP
IoT Security Architect
juanhernandez3@deloitte.com

Nihar Garg
Senior Consultant, Cyber Risk | IoT Security Architect
Deloitte & Touche LLP
IoT Security Architect
nihargarg@deloitte.com

Bin Qiu, Ph.D.
Sr. Partner SA, Deloitte | Global ER&I&Auto
Amazon Web Services
binqiu@amazon.com

Fabio Bottoni
Sr. E&U Industry Specialist SA
Amazon Web Services
fbotton@amazon.it

Pramod Daya
Sr. WW SSA IoT UKI
Amazon Web Services
dayapram@amazon.co.uk

Special Thanks

Barathi Krishnamurthy
Manager, Cyber Risk Services
Deloitte & Touche LLP
bakrishnamurthy@deloitte.com

Andrew Besley
Consultant, Cyber
Deloitte & Touche LLP
abesley@deloitte.com

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/us/about to learn more about our global network of member firms.