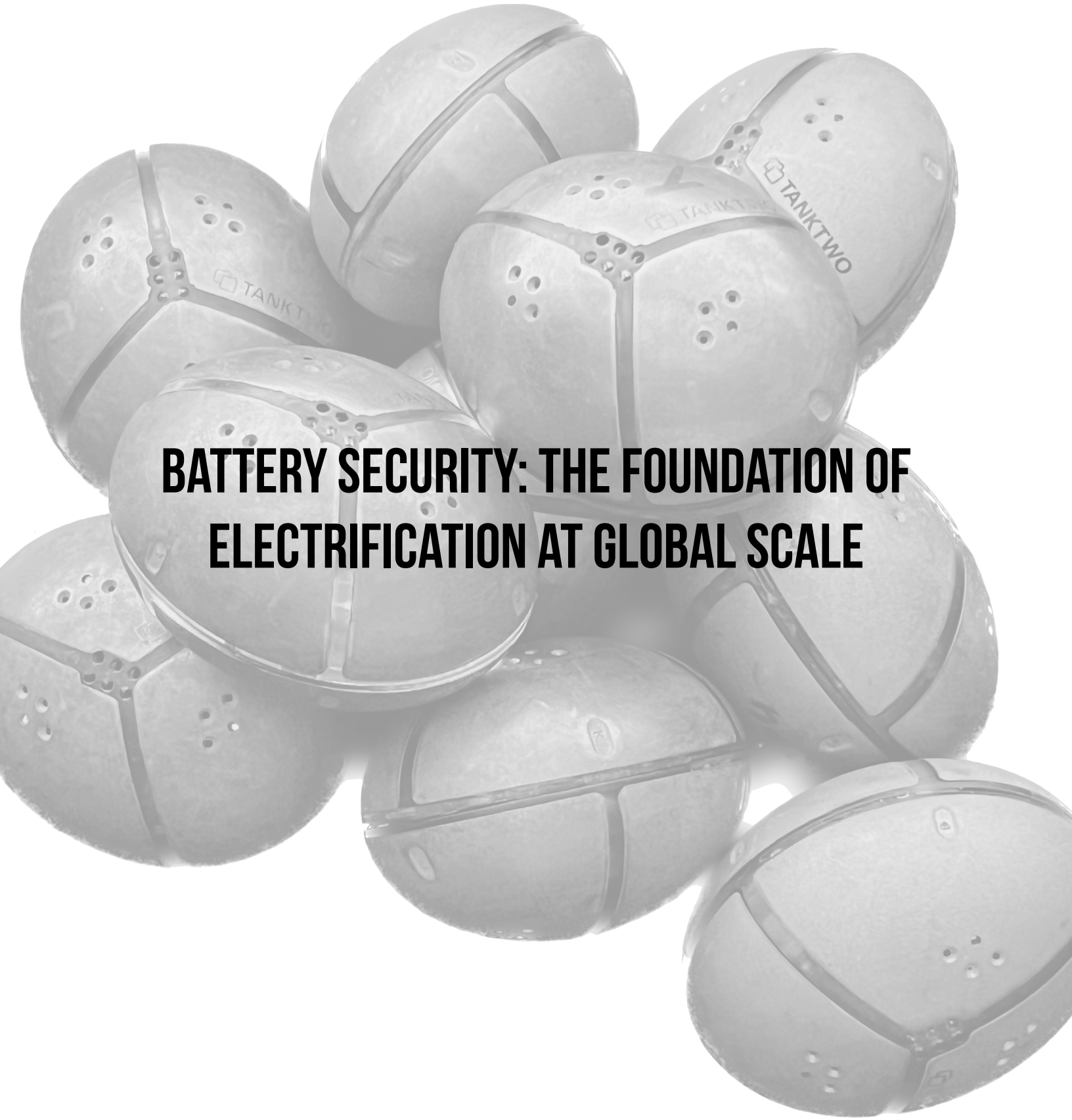


BATTERY SECURITY: THE FOUNDATION OF ELECTRIFICATION AT GLOBAL SCALE

Battery security is a complex concept. It involves a lot more than what meets the eye. As we combine technologies from various disciplines to build a revolutionary software-defined battery solution, we must consider the safety and security implications from just as many levels.

This white paper delves into the many facets of battery security — and we're just scratching the surface. Let's explore what battery security really is and isn't, why it's important in the age of accelerated electrification, and what a well-designed system can do (a lot more than preventing bad guys from blowing up EVs.)

We'll also look at the complexity of this discipline (we can spin off a few separate businesses just selling this technology) and share a high-level overview of how Tanktwo's battery security architecture works to protect high-value assets and support the electrification of critical infrastructure.

Battery security: A definition

First, let's consider the concept of security — it refers to different criteria in different contexts:

Physical security prevents access by malicious actors — the job is done when you manage to keep the bad guys out. Meanwhile, financial or social security hinges on the concept of insurance, where low-probability but high-impact events could prevent a system's continual and normal functioning.

Information and data security has a broader scope. It involves preventing access (like physical security), ensuring continuity (like social security), and promoting data integrity — e.g., by preventing unauthorized parties from modifying data in transit, authenticating user identities, and verifying the legitimacy of online entities.

Traditional battery solutions rarely include a security component. If a system does have one, it usually only addresses the physical aspect, i.e., preventing tampering by unauthorized personnel. While physical safety is important, the attack methods are much less scalable than those exploiting software weaknesses.

The advent of software-defined batteries (SDB) will change the conversation: We must expand the definition of battery security. The discipline must incorporate physical and data security with other safety measures to protect systems from intrusions and interruptions.

With great power comes great responsibility.

As such, Tanktwo's battery security architecture focuses on addressing challenges in the information security space because cyber attacks can cause widespread disruptions at unprecedented scales.

Why should we concern about battery security?

Batteries are made of expensive materials (lithium) and deliver a resource (electricity) our society relies on. Their high value means they should only be used per the contract between the owner and user(s). Battery security discourages theft by rendering a battery useless (and, therefore, worthless) when stolen.

But allowing legitimate users access is just one piece of the puzzle. These users can still do things they shouldn't — like operating the battery in dangerous conditions (e.g., too hot or too cold) or cranking up the power to an unsafe level. Such mishandling can lead to dire consequences like thermal runaways and lithium fires.

Our approach to battery security makes SDBs work as intended: It stops working for anyone who isn't authorized to use the battery system, is an authorized user but trying to do something out of contact, or takes any action that may cause physical harm (e.g., a fire.)

What does battery security cover?

Battery security ensures SDB data gets where it needs to be and makes the battery do what it needs to do but nothing more. Depending on the use case, it expands to cover ownership, safety, permitted usage, traceability of raw materials, supported business model, data integrity, and more.

We can even use battery security principles to track the carbon footprint of the energy used for charging and limit the environmental impact of the application to support broader social, environmental, and governance (ESG) goals. For example, you can configure a Tanktwo SDB to only charge from renewable sources.

Meanwhile, access control, integral to any security protocols, can expand beyond the narrower sense of safety and security to help automatically ensure the right actions are taken at the right time to maximize a battery solution's business benefits and ROI.

The importance of battery security in large-scale electrification

First, let's get onto the same page — what do we mean by large-scale electrification? In this context, it refers to the widespread implementation of large battery packs (e.g., the size of a forklift) that are not necessarily grid-tied.

Here's why a robust battery security protocol is essential for any large-scale application of software-defined battery systems:

- User safety: SDB can disable and bypass cells unsafe to operate (e.g., overheating or prone to thermal runaway.) We must ensure no one can intentionally or unintentionally tamper with this capability or alter any safety configuration.
- Critical infrastructure resiliency: Any disruption or compromise of software-defined battery systems used in critical infrastructure like power grids, hospitals, emergency services, and telecommunications could impact the reliability and continuity of these essential services.
- Cybersecurity: Besides altering the behaviors of a battery pack, hackers can use connected batteries as an entry point to infiltrate other systems and networks. Without proper security, connected battery solutions could drastically increase the attack surface.
- Access control: A battery security system can prevent unauthorized personnel from accessing or tampering with the hardware or software. You can also track who has accessed the system and what has been altered to support real-time monitoring and auditing.
- Regulatory compliance: The future of electrification will involve standards and regulations for battery safety not unlike those for cybersecurity (e.g., HIPAA, SOC 2, NIST-800). A battery security protocol will be essential for any operation to stay compliant.
- Clean energy transition and ESG compliance: Tanktwo's battery security system can track the power source used to charge the batteries. Operators can choose only green energy sources to adhere to ESG mandates.

- Electric mobility safety: Electric vehicles (EVs) can become easy targets for hackers. For example, criminals can infiltrate the system and hold a battery "hostage" for ransom. With more EVs on the road, the risks will multiply as the scale makes it more attractive for hackers to develop advanced techniques and methods.
- Public trust and investor confidence: The success of any large-scale electrification solution must gain the trust and support of the public and investors. Battery security will become a pillar in ensuring an application can achieve widespread adoption.

Battery security is essential, but building an airtight system involves numerous parties and components. Solving the complexity also brings us benefits beyond safety and security, such as providing the granular access control to accomplish other business objectives.

The complexity of battery security

A telephone from the Alexander Graham Bell era consisted of a handful of simple, easy-to-understand parts. The nerdy, 9-year-old me could take it apart and put it back together in an afternoon without my mother noticing it. I couldn't have done it with an iPhone 14 — even though both are a "telephone."

There's no such thing as an end-to-end smartphone expert — the device, discipline, and ecosystem are so vast and complex that it's practically impossible for any one person to comprehend every single element in detail (e.g., semiconductors, material science, mechanical design, UX, low-level software, databases, developer tools, privacy management, cellular, etc.)

The same is true for battery technology.

The batteries that will power large-scale electrification aren't the AA batteries you plop into a TV remote. The batteries of the future — especially those powering medical, industrial, scientific, and aerospace applications — are much closer to the iPhone than the hunk of bakelite Bell brought into the world.

Yet, many still consider batteries a single, monocultural, and siloed discipline. Battery technology isn't just about a guy in a white lab coat tinkering with battery chemistry and trying to eke out 3% more energy density in 5 years. What goes into the cells is only the acorn from which the mighty oak tree will sprout.

An advanced, software-defined battery ecosystem requires numerous players with complementary competence, including chemistry, data analytics, operations, etc. Nobody can

understand everything the entire system touches — not even those in leadership positions. As such, battery security also requires transitioning from a top-down to a horizontal structure.

Energy storage is a multi-disciplinary exercise.

As batteries become more numerous, powerful, multi-disciplinary, complex, and potentially hazardous, we have two options:

- Allow only a limited group of scientists and engineers to build and handle batteries. They must absorb an ever-growing body of specialized knowledge just to stay out of trouble and prevent everything from blowing up. Or,
- Create a framework within which specialists can contribute their expertise while putting in the guardrails so each person working in the ecosystem can't overstep their limits and make adjustments to things they don't know enough about… and blow things up.

The choice is clear if we are to scale electrification at the global level.

Maintaining checks and balances with advanced access control

Battery engineering, battery pack manufacturing, energy storage, and all the supporting functions are fast maturing. We need a competent, multi-disciplinary team to meet all the requirements. Yet, we can't have too many cooks in the kitchen, each with access to every part of the system.

Battery security creates checks and balances with various types of granular access control to ensure only the right people can manipulate the right parts of the battery system at the right time. Here's an analogy to illustrate the concept:

Let's consider a school operated by different people, including the principal, superintendent, electrician, fire marshal, treasurer, and teachers. Who should have access to the electric panel? The electrician probably gets access most of the time but not the treasurer or the teachers. That's role-based access.

What if the electrician is sick or goes on vacation? The superintendent may have temporary access to the fuse box but nothing more complex. What if there's a fire? The fire marshal should then have full access to the control panel. These instances combine role-based and event-triggered access to allow the right people to go in and do their job.

Multiply the number of players and elements by a substantial factor, and you get a glimpse of the complexity of a battery ecosystem and the security measures required to implement checks and balances.

Access control: Beyond safety and security

Access control is integral to battery security, but it goes beyond ensuring safety, safeguarding data, and fending off hackers. The technology also makes it possible to control and optimize resource usage. Here's an example:

The school principal told the groundskeeper that he can't mow the lawn on Tuesdays from 2 to 4 pm because… oboe practice. But what if the groundskeeper has a problem following schedules?

Let's say the school replaces its fume-spewing John Deere with a TBOS-powered mower. The principal can simply disable the mower battery on Tuesdays from 2 to 4 pm on the west side of the building (using geofencing) by clicking a few buttons on a software interface.

You can also set the battery system to automatically pull time information from the school's centralized scheduler so the lawn mower will not work whenever there's an oboe practice. The rule-based control means administrators only need to update the policy once to enforce it through every battery in the network to ensure compliance.

But how can you ensure the lawn mower battery only takes directions from authorized personnel? TBOS's battery security architecture provides authentication and verification capabilities to ensure the software only follows commands from legitimate sources.

Let's go further and look beyond the narrower definition of security. Say, the leasing company has determined that the SDB's maximum discharge level is 30% since lower discharge limits can adversely impact battery longevity. The battery can retain 98% of its original capacity when the lease is up in 24 months, and the company can sell it for good money.

As it turns out, the groundskeeper can mow 7 out of the school's 8 acres on one charge. But he has to return to the shed and charge the machine to finish the job, costing the school an estimated $20 in productivity per week, or $80 per month — presenting a business opportunity to the leasing company.

If it changes the depth of discharge (DoD) limit from 30% to 15% so the battery can hold more charge, the groundskeeper can mow all 8 acres in one go. However, lowering the DoD limit

causes more wear and would reduce the residual value of the battery at the end of the leasing period by $240, or $10 a month.

The leasing company proposes an increase of $25 per month on the lease for the school to gain $80 in productivity. It's a no-brainer: the school saves $65 per month, and the leasing company makes $15 more monthly. They agree on the arrangement, and the leasing company changes the parameters via the software interface.

The underlying principle and mechanisms of our battery security system facilitate this business model to make asset and revenue optimization possible. They provide a method for involved parties to enter permission, schedule, location, authorizations, dependencies, and other business data to automate the execution of strategies and policies.

TBOS: Sandboxing for secure battery development and operations

Battery security lives at the intersection of data science, cryptography, material science, and economics and is the foundation on which we build SDB, the battery topology of the future. It's the cornerstone of the Tanktwo Battery Operating System (TBOS) and is interwoven with all TBOS's capabilities.

Our battery security architecture allows organizations, systems, or teams with specific competence to work in their areas of expertise (i.e., sandboxes) while interacting with adjacent ones to ensure seamless integration of different functionalities without the ability to alter things they don't know enough about.

The sandboxing arrangement facilitates collaboration among experts in various disciplines to optimize each application. For example, an owner will likely want to maximize the lifespan of the asset (i.e., battery pack) but don't have the knowledge to know how far to turn the dial before safety or accelerated wear becomes an issue.

With advanced access control mechanisms, our technology sandboxes different functional areas. For instance, the owner can interact with battery chemistry experts to optimize asset lifespan, safety, and operational simplicity to maximize lifetime value without impacting safety. Non-specialists can operate the system independently without jeopardizing its integrity.

Sandboxing requires an airtight cryptography-based ecosystem, and we have integrated it into TBOS's battery security architecture. We build the security part of this foundation on operational principles to support the universal long-tail implementation of electrified products and equipment.

Battery security allows the right people to access the right capabilities

With our battery security architecture, different players in the battery ecosystem can perform their duties or optimize business outcomes without blowing things up or exposing the architecture to external threats.

- Business decision-makers can develop products and pricing structures to support business models without straining a battery's capacity.
- Battery chemistry experts can change limits for cell temperature, voltages, currents, waveforms, duty cycles, etc., to support business requirements.
- Fleet managers can re-allocate battery packs across vehicles and drivers to access extra power (i.e., "turbo boost") when required.
- Utility companies can use battery packs for buffer capacity when the grid is strained (at a predetermined cost.)
- Power-as-a-Service providers can limit the performance or shut down the power supply when a customer skips payment.
- Insurance providers can limit how and where a battery pack is used (e.g., with geo-fencing.)

Battery security also prevents:

- Battery packs from self-discharging and becoming unusable.
- Black market economies from re-purposing batteries.
- Drivers from using "turbo boost" too often, compromising the battery packs' longevity.
- Lessees from using batteries in geographic areas outside their service agreements (e.g., places that are too hot or cold, which may affect battery health and safety.)
- Owners from getting back battery packs with worse state-of-health than anticipated at the end of a lease agreement.

How Tanktwo battery security technology works

Apple is an example of how hardware and software security support each other. You can steal an iPhone, but the iCloud lock is so secure that you can't do much with the hardware. To use an iPhone, you need physical access to the device. And the software layer controls the rights to use it.

Like how a stolen iPhone doesn't get you very far, unauthorized users can't activate a stolen TBOS-powered battery. What's left is an expensive, 500-pound doorstop.

We build our battery security approach on existing security principles, but the multidimensionality of the discipline makes it complex and challenging to execute:

1. Companies must translate contractual, practical, and operational principles or guidelines into a playbook for the technology to execute. (Like the lawnmower example.)
2. They must support the system with information security implementation to provide the abstract limitation, permission, and authorization to support #1.
3. They must support the software commands with electronic-based hardware implementation. After all, airtight information security is worthless if a threat actor can bypass the security system through hardware weaknesses.

To help product builders and service providers overcome the complexity of battery security, we build the entire architecture into TBOS and abstract it from the battery system's application.

The plug-and-play solution allow you to customize this security layer and sandwich it between any battery system and application. You can also update it via software to ensure ongoing compliance with changing guidelines, business requirements, and regulations.

Our software architecture uses the internet's security backbone to protect access to battery systems with digital keys and certificates. The multidimensional approach involves many components, which intertwine to create a multi-layered web to address physical and cyber threats. Here's an overview of these principles:

Battery security key management

Key management is the most critical principle behind battery access control and sandboxing. It's the process of generating, distributing, storing, and revoking cryptographic keys for securing communications in various information systems to ensure data confidentiality, integrity, and authenticity.

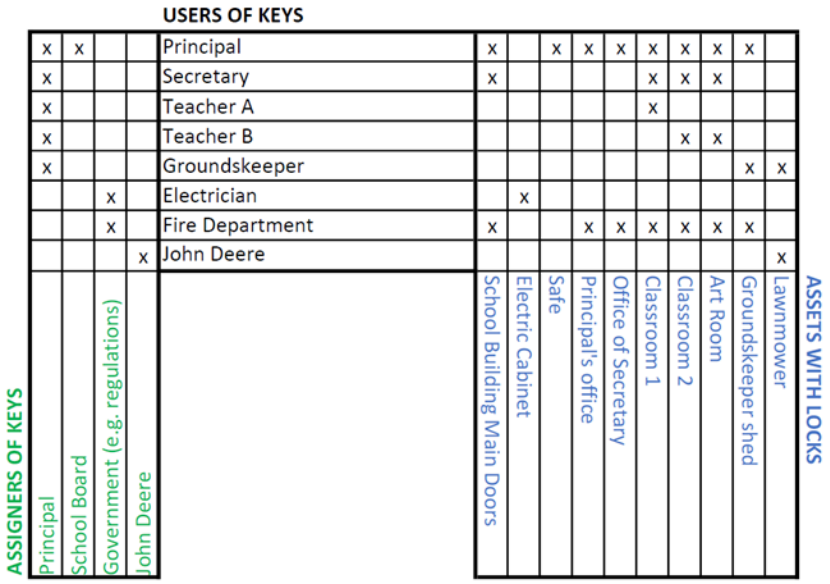
Let's illustrate the key management concept with the school example:

Various users (e.g., principal, secretary, groundskeeper) have different job functions and need to access various locked assets to do their job. Each user is issued a set of keys to perform their duty:

USERS OF KEYS	School Building Main Doors	Electric Cabinet	Safe	Principal's office	Office of Secretary	Classroom 1	Classroom 2	Art Room	Groundskeeper shed	Lawnmower
Principal	x		x	x	x	x	x	x	x	
Secretary	x					x	x	x		
Teacher A						x				
Teacher B							x	x		
Groundskeeper									x	x
Electrician		x								
Fire Department	x			x	x	x	x	x	x	
John Deere										x

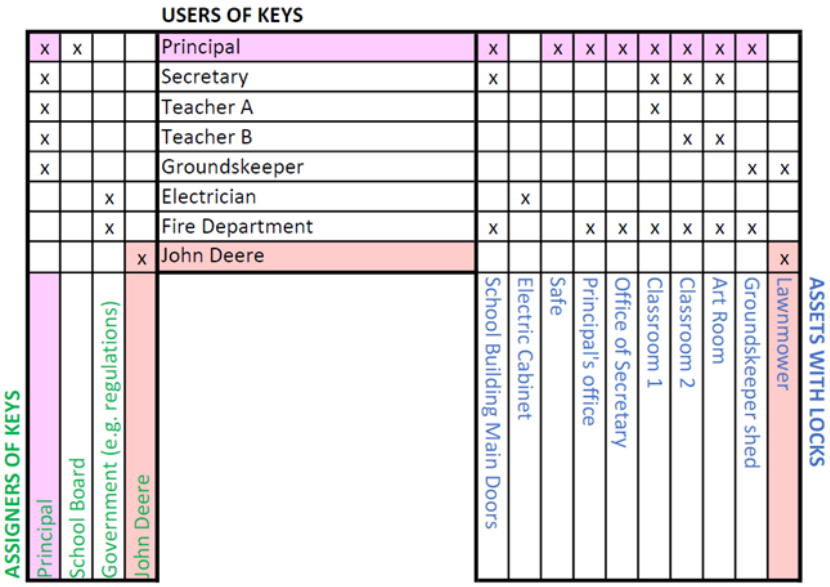
ASSETS WITH LOCKS

But who decides which role gets which keys? We must define people or entities authorized to assign keys:



ASSIGNERS OF KEYS: Principal	ASSIGNERS OF KEYS: School Board	ASSIGNERS OF KEYS: Government (e.g. regulations)	ASSIGNERS OF KEYS: John Deere	USERS OF KEYS	ASSETS WITH LOCKS: School Building Main Doors	ASSETS WITH LOCKS: Electric Cabinet	ASSETS WITH LOCKS: Safe	ASSETS WITH LOCKS: Principal's office	ASSETS WITH LOCKS: Office of Secretary	ASSETS WITH LOCKS: Classroom 1	ASSETS WITH LOCKS: Classroom 2	ASSETS WITH LOCKS: Art Room	ASSETS WITH LOCKS: Groundskeeper shed	ASSETS WITH LOCKS: Lawnmower
x	x			Principal	x		x	x	x	x	x	x	x	
x				Secretary	x					x	x	x		
x				Teacher A						x				
x				Teacher B							x	x		
x				Groundskeeper									x	x
		x		Electrician		x								
		x		Fire Department	x			x	x	x	x	x	x	
			x	John Deere										x

However, we run into weaknesses when the key issuer and key user overlap. For instance, John Deere has been reluctant to issue keys to users to enable equipment repair — leading to major headaches for the parties involved and illustrating how a well-designed key management system is essential for the proper functioning of the ecosystem.



ASSIGNERS OF KEYS: Principal	ASSIGNERS OF KEYS: School Board	ASSIGNERS OF KEYS: Government (e.g. regulations)	ASSIGNERS OF KEYS: John Deere	USERS OF KEYS	ASSETS WITH LOCKS: School Building Main Doors	ASSETS WITH LOCKS: Electric Cabinet	ASSETS WITH LOCKS: Safe	ASSETS WITH LOCKS: Principal's office	ASSETS WITH LOCKS: Office of Secretary	ASSETS WITH LOCKS: Classroom 1	ASSETS WITH LOCKS: Classroom 2	ASSETS WITH LOCKS: Art Room	ASSETS WITH LOCKS: Groundskeeper shed	ASSETS WITH LOCKS: Lawnmower
x	x			Principal	x		x	x	x	x	x	x	x	
x				Secretary	x					x	x	x		
x				Teacher A						x				
x				Teacher B							x	x		
x				Groundskeeper									x	x
		x		Electrician		x								
		x		Fire Department	x			x	x	x	x	x	x	
			x	John Deere										x

As such, we must introduce another layer in our battery security architecture to provide checks and balances.

This example matrix describes which key turners can unlock which battery capabilities and which entities can issue keys:

"TURNERS OF KEYS" TO A BATTERY	Limp Mode	On/Off switch	Renewable Source Requirement	Geographic Fencing	Target Application Setting	Min/Max Temp range setting	Min/Max SoC level setting	Max Charge Speed Setting	Max Discharge speed setting	Min/Max voltage setting
Application (e.g. vehicle)		x								x
Driver		x								
Fleet Manager		x			x					x
Courier Company		x	x	x	x					
Leasing Company/Owner	x	x		x	x	x	x	x	x	x
Cell Chem data specialist	x					x	x	x	x	
Power company			x					x		
Tanktwo		x			x	x	x	x	x	x

BATTERY ASSETS WITH LOCKS

ASSIGNERS OF KEYS			"TURNERS OF KEYS" TO A BATTERY	Limp Mode	On/Off switch	Renewable Source Requirement	Geographic Fencing	Target Application Setting	Min/Max Temp range setting	Min/Max SoC level setting	Max Charge Speed Setting	Max Discharge speed setting	Min/Max voltage setting
Courier Company/Customer	Leasing Company/Owner	Tanktwo											
x			Application (e.g. vehicle)		x								x
x			Driver		x								
x			Fleet Manager		x			x					x
	x		Courier Company/Customer		x	x	x	x					
	x		Leasing Company/Owner	x	x		x	x	x	x	x	x	x
	x		Cell Chem data specialist	x					x	x	x	x	
x			Power company			x					x		
x	x	x	Tanktwo		x			x	x	x	x	x	x

BATTERY ASSETS WITH LOCKS

But how do you prevent the key assigners from turning on "god mode" and doing whatever they want?

The check and balances come from a traditional commercial contractual agreement, stating the roles and responsibilities of each party. In the example above, the courier company (the customer) has the intrinsic rights to:

- The vehicle, which it owns.
- The driver and fleet managers, typically through an employment contract.
- The power company (e.g., that supplies green energy.)

The courier company also has a licensing agreement with Tanktwo to use our SDB technology to power its fleet.

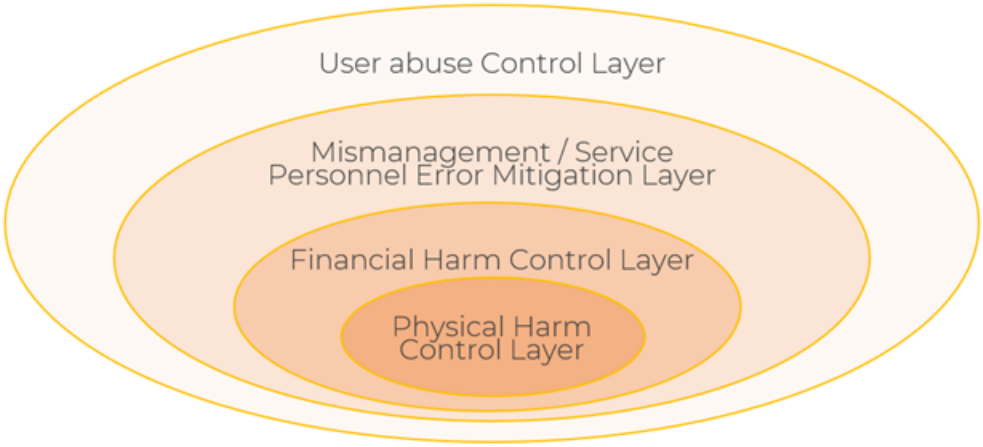
Meanwhile, the leasing company is the legal owner of the battery and has traditional commercial contracts with its customer (i.e., the courier company) and a cell data specialist to optimize cell performance and fine-tune battery parameters. It also has a standard license agreement with Tanktwo to use our technology in their batteries.

The critical component is the ability to turn the contractual principles into a set of rules that the technology can execute — and we built our algorithms from the ground up to support this capability.

The battery security onion

What guides keys issuance in battery management? The more potential harm an action can cause, the fewer people should have the power to execute that action.

To that end, we establish keys for roughly four layers/categories: User abuse control, mismanagement or service personnel error mitigation, financial harm control, and physical harm control to leverage advanced principles of proven operating systems.



Here's what the layers in the battery security onion mean, in oversimplified terms:

- If you don't know what you're doing and are poking around in the innermost circle, you could cause a fire or explosion. The risk of personal harm is high if anything goes wrong here.
- If you don't know what you're doing and have access to the "financial harm control" layer, you could cause irreparable damage. But you will probably survive.
- If you're an incompetent maintenance shop manager playing in the "service personnel mitigation" layer, you may prevent the electric buses from going out the following day and get yourself fired.
- If you're a regular human, the "user abuse control" is for you. This layer covers behaviors like slamming an electric truck into reverse at 70mph — it shouldn't happen, but someone will do it someday. But ideally, not too many things break.

The battery security onion informs the level of access control to implement — i.e., who should be allowed to touch what. It's critical because in battery technology, a tiny typo could lead to disastrous consequences.

Let's say the cell chemistry data specialist with access to the innermost layer determined that raising the maximum cell charging voltage from 4.20V to 4.25V is safe. But they make a typo and key in 5.25V. Without the appropriate checks and balances, the error will lead to a violent battery fire the next time someone charges the pack.

That's why our battery security architecture prohibits actions that could cause physical harm altogether and protect specific parameters and actions with a belt-and-suspender approach — requiring more than one key to unlock a function:

x: "either/or"
x: "all parties required"

ASSIGNERS OF KEYS: Courier Company/Customer	Leasing Company/Owner	Tanktwo	"TURNERS OF KEYS" TO A BATTERY	Limp Mode	On/Off switch	Renewable Source Requirement	Geographic Fencing	Target Application Setting	Min/Max Temp range setting	Min/Max SoC level setting	Max Charge Speed Setting	Max Discharge speed setting	Min/Max voltage setting
x			Application (e.g. vehicle)		x								x
x			Driver		x								
x			Fleet Manager		x			x					x
	x		Courier Company/Customer		x	x	x	x					
	x		Leasing Company/Owner	x	x		x		x	x	x	x	x
	x		Cell Chem data specialist	x					x		x		
x			Power company			x					x		
x	x	x	Tanktwo		x			x	x	x	x	x	x

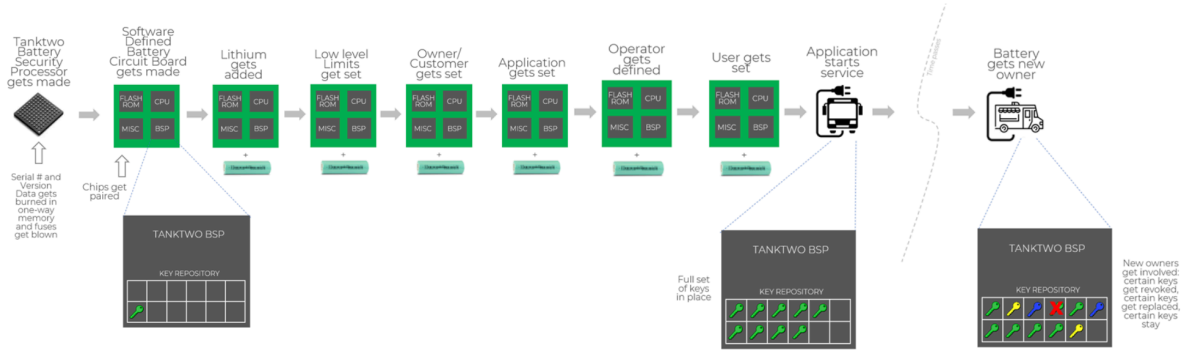
BATTERY ASSETS WITH LOCKS

In the above example, the min/max state of charge (SoC) setting requires sign-off by the leasing company (the owner) and the cell chemistry data specialist because the decision involves deep battery chemistry knowledge and insights into the financial implication (since widening the SoC window can accelerate deterioration and impact the remaining useful life.)

The Tanktwo battery security processor: Layering battery security fundamentals

The TBOS security system starts with the battery security processor (BSP). We burn the serial number and version data into the chip write-once memory, which can't be altered afterward in any way. Then, we add the BSP to the SDB circuit board, where it's paired with other chips (e.g., CPU, flash ROM.)

Next, we layer down different components — like adding the lithium and setting some low-level limits (e.g., temperature and current limits). Then, we define details about the owner, application, operator, and user — adding keys to the key repository for granular access control, authentication, etc. (e.g., who can access or change which function and under what circumstances.)



When the battery changes ownership, we can adjust the set of keys to change access privilege and other security perimeters by revoking, rewriting, or substituting existing ones.

The BSP contains several types of key repositories: write once, read many; write once, read never; write-until-write protected, and rewritable — allowing us to balance security, granularity, and flexibility.

Battery security in the age of accelerated electrification

Electrification is transforming numerous industries and is pivotal in shaping our energy landscape. But current battery technology has many limitations, which prevent us from reaching the tipping point in the clean energy transition.

Software-defined batteries address these challenges and limitations. However, the same capabilities also introduce new concerns.

For SDB systems to communicate with centralized control, transmit data for analytics and real-time optimization, and receive commands to change behaviors on the fly — they must be connected to a network (e.g., the internet.)

But any time you plug something into a network, it becomes hackable and the owners become extortable. Now you may wonder, we've lived in a connected world long enough — why hasn't this been a concern?

While many expensive physical assets already have some form of digital control and supervision (e.g., SCADA), few are connected to the internet because of severe security risks. Techniques like air-gapping (i.e., not connecting an asset to the internet) increase the physical effort required to breach a system, which has often been enough to deter attacks at scale.

But as we have learned from the Stuxnet computer worm, if the target is high-value enough, hackers can find ways to breach the air gaps. Today, we're seeing a fast-growing number of air-gap-crossing attacks, and we can no longer rely on air gaps to provide sufficient security.

Meanwhile, the numerous digital and connected devices are generally of low value. So even though the security of most IoT devices is virtually non-existent (hackers can get into your home network through the thermostat or use your smart lightbulb to power their botnets), we aren't seeing widespread, devastating impacts — yet.

But things are about to change as AI enters the game, making it much faster and easier for criminals to go after the long tail of hackable devices. The business case/ROI of hacking will change, and things that aren't considered security risks today will soon become liabilities.

To understand the impact of digital attacks on expensive physical assets like connected battery systems, think back to the earlier days of cybersecurity. The threat landscape was the wild west, and the lack of awareness made many organizations easy targets.

Now, the only difference is that criminals have already developed advanced techniques to infiltrate software systems. They don't need to figure them out from square one. Battery solutions running on software without iron-clad security measures are simply sitting ducks.

Electrification of critical infrastructure

In March 2023, the White House published an updated National Cybersecurity Strategy. Pillar one concerns the defense of critical infrastructure. The incapacitation or destruction of these physical or virtual assets, systems, and networks would have a debilitating effect on security, the national economy, and/or public health and safety.

The 16 critical infrastructure sectors covered by the mandate are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergence services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors and waste, transportation systems, and water and wastewater systems.

Many of these sectors are also entering the electrification revolution. Advances in battery technology, such as SDB, will enable the transition to clean energy at unprecedented speed and scale. But the connectivity will also leave many critical systems open to exploitation if proper security measures are lacking.

Without an airtight battery security protocol, electrification of these critical infrastructure sectors at scale won't be feasible.

A security-first mindset for the future of electrification

SDBs will drive the future of electrification. But airtight battery security is the prerequisite: (1) To enable a multi-disciplinary team to participate and collaborate safely through sandboxing and access control; (2) To prevent bad actors from breaching these systems, including critical infrastructure, for criminal activities.

Now you may wonder, what could go wrong? Since battery systems are expensive physical assets connected to digital networks, attacks could take many shapes and forms. For example, threat actors can launch ransomware, DDoS, or supply chain attacks — like the Colonial Pipeline incident but on a much larger scale.

Criminals can also venture into a new realm — they may steal power, over-stress batteries, "tune/overclock" batteries, reprogram serial numbers to make stolen packs appear legitimate (like a digital VIN swap,) break geofencing locks, make cells look like they have fewer cycles (like odometer rollback,) or cause other types of financial harm.

Additionally, lithium-ion battery packs contain vast amounts of energy. Criminals could program them to short out and cause a fire unless a ransom is paid. We aren't just talking about the high cost of data breaches (which can also happen) but a public safety risk.

Tanktwo battery security stays ahead of the game

Battery security isn't an afterthought in TBOS. We developed our system from the ground up with the BSP as an integral part of the software architecture.

But we stay ahead of the game not by claiming that we'll make software without vulnerabilities. Despite the most rigorous development and testing process, we know our software has (yet to be discovered) bugs and problems — like any application on the planet. We also don't believe in the fallacy of security through obscurity.

We stay ahead by adhering to the latest and strictest software design, data management, and security best practices. We review and re-review our code and invite experts to inspect our

security-critical documentation. We're planning a bounty program to reward white hat hackers who can break our code and show us our vulnerabilities.

Most importantly, we keep a close eye on all types of vulnerability disclosures across multiple industries because of the breadth and depth of our system.

We built TBOS by combining various tried-and-true technologies, which have been proven for the past 10, 20, or 30 years. We leverage best-in-class technologies as much as possible without reinventing the wheel — which means we have security experts globally to watch for vulnerabilities and devise solutions.

For example, we monitor the Common Vulnerabilities and Exposures (CVE) database lists. If any technology we use has a suspected vulnerability, we'll immediately analyze its relevance and address the issue.

We can't afford not to transition to clean energy, and SDB will unlock electrification at scale. Like we won't stop using the internet because of cyber threats, we shouldn't stop the progress of electrification because of security concerns. By combining best practices from multiple industries to create the safest and most cost-efficient power system, TBOS offers the solution to drive the future of electrification.