A TISAX követelmények áttekintése

Dr. Horváth Zsolt

Kivonat

A TISAX® (Trusted Information Security Assessment Exchange, azaz magyarul: Megbízható Információbiztonsági Értékelések Megosztása) egy olyan autóipari információbiztonsági rendszer, amely az ISO/IEC 27001 információbiztonsági szabványt nemcsak kiegészíti, hanem egyben annak használatát is lényegesen szigorúbbá teszi az autóipari szereplők számára. Az elmúlt években általános információbiztonsági és TISAX-os tanácsadásaink során gyakran azt tapasztaltuk, hogy sok vállalat indulásban nemhogy a TISAX követelményeit, de még az általános és alapvető információbiztonsági követelményeket is csak alig ismeri. Ilyen esetekben a TISAX-nak megfelelő információbiztonsági rendszer kiépítése jellemzően nem egy meglévő és működő információbiztonsági rendszer kiegészítését jelenti a TISAX által meghatározott további követelmények alapján, hanem az információbiztonsági alapoktól való indulást. Ezért is fontos annak megértése, hogy egy információbiztonsági rendszer – különösen a TISAX – bevezetése mivel is jár egy vállalat életében.

Jelen publikáció áttekintés szintjén mutatja be a TISAX követelményrendszerének fő struktúráját és szakmai elemeit, segítve ezzel az azt alkalmazni kívánó vállalatokat a kezdeti döntések meghozásában.

Bevezetés

A TISAX®[1] autóipari információbiztonsági követelményrendszer elfogadottsága a 2017-es bevezetése óta folyamatosan nőtt. Noha a TISAX a bevezetését követő első években még alig volt ismert, 2021 év végére már több mint 4000 TISAX megfelelési igazolás volt érvényben, melyekből kb. 30-40 már magyarországi telephelyekre vonatkozott. Magyarországon a legtöbb autóipari beszállító vállalat már találkozott ezzel a követelménnyel, komolyabban azonban csak kevesen kezdtek el foglalkozni vele.

A TISAX fokozatos bevezetése során a közeljövőben várható az az időszak, amikor már általánossá válik, hogy az autóipari gyártók (OEM-ek) kötelezővé teszik beszállítóik számára a TISAX teljesítését. Magyarországon például az Audi Hungária Zrt. a beszállítói oldalán közzétett Általános Információtechnoló-

[1] TISAX = Trusted Information Security Assessment Exchange, azaz magyarul: Megbízható Információbiztonsági Értékelések Megosztása

giai Feltételek (ÁIF) [1] részeként az alvállalkozóktól elvárt információbiztonsági követelmények között előírja a TISAX-nak való megfelelési igazolás meglétét is.

2020 júniusában megjelent publikációmban [2] bemutattam a TISAX információbiztonsági rendszer célját, az ENX szervezet[2] általi működtetés kereteit, valamint áttekintést adtam a TISAX-ot alkalmazni kívánó vállalatok számára a legfontosabb szükséges lépésekről. Azóta a kezdeti tapasztalatok felhasználásával a követelményrendszert is továbbfejlesztették, így annak további verziói jelentek meg. Jelen publikációban ennek fontosabb változásait szeretném bemutatni, valamint áttekintést adni a jelenlegi TISAX követelmények főbb szakterületeiről.

Kisebb változások a TISAX folyamatban

A TISAX rendszer alapvető működését az ENX a saját honlapján, a TISAX Résztvevői Kézikönyvben [3] teszi közzé a felhasználó vállalatok számára. A TISAX alapvető működése, a regisztráció folyamata, az értékelés (audit), illetve az arra való felkészülés folyamata, továbbá az eredményeknek az ENX portálon történő megosztása lényegében ugyanolyan, mint ahogy az az előző publikációban [2] már bemutatásra került. A TISAX Résztvevői Kézikönyv új verziójában létrejött kisebb változások elsősorban az értékelési követelményrendszer fontosabb változásaihoz történő kiigazításokat tartalmazzák.

Egyik fontos változás, hogy a TISAX értékelési követelményrendszerében (ISA) megszűnt a „Csatlakozás harmadik felekhez" című önálló terület, így a választható értékelési célok száma lecsökkent 10-ről 8-ra. A választható értékelési célok lehetnek:

1. Magas védelmi igényű információk
2. Nagyon magas védelmi igényű információk
3. Prototípus alkatrészek és részegységek védelme
4. A jármű prototípus védelme
5. Tesztjárművek kezelése
6. Prototípusok védelme rendezvények, film- vagy fotózás közben
7. Adatvédelem
8. Adatvédelem a személyes adatok különleges kategóriáival

A szükséges értékelési cél a vállalati tevékenység alapján határozható meg. Az első, a „Magas védelmi igényű információk" értékelési cél követelményei alapvetőnek számítanak, azt minden TISAX rendszerben teljesíteni kell. Prototípussal kapcsolatos értékelési célt akkor szükséges választani, ha az adott beszállító tevékenysége konkrét prototípus termékekkel vagy alkatrészekkel kerül kapcsolatba. Ez lehet például egy adott prototípus alkatrész gyártása, próbajárművek tesztelése, vagy akár új prototípus berendezések hivatalos sajtóbemutatóinak szervezése, lebonyolítása is. Az adatvédelemmel kapcsolatos értékelési célok a személyes adatok kezelésére vonatkoznak, és olyan esetekben szükséges azt választani, amikor a beszállító szolgáltatásának tárgya a megrendelő vállalat alkalmazottai személyes adatainak kezelése. Ilyen szolgáltatás lehet például egy megrendelő vállalat számára működtetett e-learning rendszer üzemeltetése.

[2] ENX szervezet = European Network Exchange Association

Az értékelési célok tehát a beszállítás vagy szolgáltatás tárgyához kapcsolódnak, és tulajdonképpen azt határozzák meg, hogy a TISAX követelményrendszer mely moduljainak kell megfelelni. Amennyiben az értékelési célok meghatározása nem egyértelmű a vállalat számára, akkor ajánlott előre egyeztetni a megrendelővel, hogy melyik értékelési cél teljesítését várja el az adott beszállítóval való szerződéskötéshez.

Az értékelési célok kiválasztása kapcsolatban van még az elvárt védelmi szinttel és az értékelési szinttel (AL – Assessment Level) is. Ezek kapcsolatát az 1. táblázat [3] mutatja.

No.	A TISAX értékelési cél	Védelmi szint	Értékelési szint
1.	Magas védelmi igényű információk	magas	AL 2
2.	Nagyon magas védelmi igényű információk	nagyon magas	AL 3
3.	Prototípus alkatrészek és részegységek védelme	magas	AL 3
4.	A jármű prototípus védelme	magas	AL 3
5.	Tesztjárművek kezelése	magas	AL 3
6.	Prototípusok védelme rendezvények, film- vagy fotózás közben	magas	AL 3
7.	Adat védelem. Az európai általános adatvédelmi rendelet (GDPR) 28. cikke („Adatfeldolgozó”) szerint	magas	AL 2
8.	Adatvédelem a személyes adatok különleges kategóriáival A 28. cikk („Adatfeldolgozó”) szerint a személyes adatok különleges kategóriáival, az európai általános adatvédelmi rendelet (GDPR) 9. cikkében meghatározottak szerint	nagyon magas	AL 3

1. táblázat: A TISAX értékelési célok kapcsolata az ISA védelmi szintekhez és a TISAX értékelési szintekhez

A védelmi szint lehet „magas” vagy „nagyon magas” besorolású, melyek a TISAX értékelési követelményrendszerben az egyes témakörökhöz kapcsolódó magas vagy nagyon magas védelmi igényű információk további kiegészítő követelményeinek teljesítését írják elő.

A TISAX értékelési szint (AL) az értékelés, azaz az audit szintjét határozza meg, és az audit lefolytatásának módjára vonatkozik. Ez alapvetően három értéket vehet fel: AL1, AL2 és AL3. Ezek jelentése:

1. AL1 – Assessment Level 1: csak a szervezet saját önértékelése történik, az auditor csak a témák meglétének teljességét vizsgálja, tartalmát azonban nem. Egyszerűbb esetekben ez is elégséges lehet, ENX TISAX megfelelési igazolás viszont nincs ehhez a szinthez.

2. AL2 – Assessment Level 2: az értékelés során az önértékelés eredményeinek „hihetőségi vizsgálata” a benyújtott dokumentációk és bizonylatok alapján, alapvetően dokumentációértékelés távaudit módszerrel, helyszíni vizsgálat csak szükség esetén történik.
3. AL3 – Assessment Level 3: teljes és részletes helyszíni audit folyamat, a bizonyítékok ellenőrzésével és interjúkkal lefolytatva.

Az 1. táblázat azt mutatja meg, hogy a TISAX megfelelés igazolásához az egyes értékelési célok választása esetén minimum milyen értékelési szintű audit lefolytatása szükséges.

Egy másik fontos változás a követelményekben, hogy mindegyik terület, folyamat elvárt érettségi szintje egységesen a 3-as szint, ami az érettségi modellben a sztendertizált folyamatok működtetését jelenti.

A TISAX követelményrendszer változásai

Az értékelési követelményeket az ENX a saját honlapján, az Információbiztonsági értékelés c. Excel táblázatban (ISA) [4] teszi közzé a felhasználó vállalatok számára. Ez a táblázat tartalmazza azt a csekklistát, amely alapján a TISAX-ot felülvizsgáló szervezet értékeli (auditálja) majd a vállalat információbiztonsági rendszerét, és a vállalatnak is ugyanezen csekklista követelményeinek teljesítésével kell felkészülnie az auditra. Tehát ez a táblázat tartalmazza a TISAX megfelelési követelményeket és elvárásokat.

A követelmények rendszerezése, struktúrája az 5. főverzióban lényegesen megváltozott, és könnyebben áttekinthetővé, érthetőbbé vált. A vállalat tevékenységétől függően (a TISAX értékelési célnak megfelelően) kell meghatározni, hogy az ISA mely követelménymodulját kell alkalmazni. Az ISA táblázat három külön munkalapon tartalmazza a teljesítendő követelményeket. Ezek a következők:

- Információbiztonság. (Ez az alap csekklista, kitöltése minden esetben kötelező.)
- Prototípus védelem. (Opcionális, csak a megfelelő auditcél esetén kitöltendő, ott is a cél határozza meg, hogy melyik részét szükséges kitölteni.)
- Adatvédelem. (Opcionális, csak a megfelelő auditcél esetén kitöltendő.)

Az „**Információbiztonság**” c. modul hét fő biztonsági témakör szabályozásait írja elő, a következő biztonsági alterületi bontásokban:

1. Információbiztonsági szabályozások és szervezet
   a. Információbiztonsági szabályzatok
   b. Az információbiztonság szervezete
   c. Vagyonelemek kezelése
   d. Információbiztonsági kockázatmenedzsment
   e. Értékelés (audit)
   f. Incidenskezelés
2. Humán erőforrások
3. Fizikai biztonság
4. Azonosítás és hozzáférés
   a. Azonostás menedzsment
   b. Hozzáférés felügyelet
5. Informatikai biztonság / kiberbiztonság
   a. Kriptográfia (titkosítás)
   b. Üzemeltetés biztonsága
   c. Kommunikáció biztonsága
6. Beszállítói kapcsolatok
7. Megfelelés

A modul ezekre a területekre határoz meg 41 folyamatot, amelyre folyamatonként meghatározott a folyamat célja és a teljesítendő 5-15

követelmény. Ezek együttesen többszáz követelményt tartalmaznak, amelyek négy kategóriába vannak besorolva:

- „kötelező" követelmény, amelyet a folyamat működtetése esetén minden esetben teljesíteni kell;
- „ajánlott" követelmény, amelyet a folyamat működtetése esetén nagyon ajánlott teljesíteni, csak nagyon alapos indoklással lehet eltekinteni tőle;
- „magas védelmi igényekre" vonatkozó további követelmények, amelyeket az adott folyamat kapcsán a magas védelmi igényű adatok kezelése esetén kell alkalmazni;
- „nagyon magas védelmi igényekre" vonatkozó további követelmények, amelyeket az adott folyamat kapcsán a nagyon magas védelmi igényű adatok kezelése esetén kell alkalmazni (csak a 2. és a 8. értékelési cél esetén kötelező a használata);

A modul teljesítése mindegyik TISAX rendszer esetén kötelező. A fenti területek minden folyamatát olyan módon kell szabályozni, hogy az a folyamatokhoz meghatározott összes követelményt mind teljesítse, és a folyamat szabályozott és dokumentált működése megfeleljen a 3. érettségi szintnek.

A „**Prototípus védelem**" c. modul öt fő biztonsági témakör szabályozásait írja elő:

1. Fizikai és környezeti biztonság
2. Szervezeti követelmények
3. A járművek, alkatrészek és részegységek kezelése
4. A próba-járművekre vonatkozó követelmények
5. Az eseményekre és a fotózásokra vonatkozó követelmények

A modul ezekre a területekre határoz meg 22 folyamatot, amelyre folyamatonként meghatározott a folyamat célja és a teljesítendő 5-10 követelmény. Ezek is együtt több, mint száz követelményt tartalmaznak, amelyek három kategóriába vannak besorolva:

- „kötelező" követelmény, amelyet a folyamat működtetése esetén minden esetben teljesíteni kell;
- „ajánlott" követelmény, amelyet a folyamat működtetése esetén nagyon ajánlott teljesíteni, csak nagyon alapos indoklással lehet eltekinteni tőle;
- „a védelmet igénylőnek minősített járművekre" vonatkozó kiegészítő követelmények, amelyeket az adott folyamat kapcsán a védelmet igénylőnek minősített járművekre vonatkozóan kell alkalmazni (ezek jellemzően a fizikai biztonság témakörében a védelmet igénylő járművek elhelyezésének különleges biztonsági szempontjaira vonatkoznak).

A modul teljesítése csak a 3-6. számú TISAX értékelési célok esetén kötelező, ahol azt is az értékelési cél határozza meg, hogy a „Prototípus védelem" modul melyik területeinek követelményei teljesítendők. Ugyanakkor – hasonlóan az „Információbiztonság" modulhoz – a teljesítendő területek minden folyamatát olyan módon kell szabályozni, hogy az a folyamatokhoz meghatározott összes követelményt mind teljesítse, és a folyamat szabályozott és dokumentált működése megfeleljen a 3. érettségi szintnek.

Az „**Adatvédelem**" c. modul mindössze négy kérdéskört tartalmaz, amely az európai általános adatvédelmi rendelet (GDPR) megfelelő fejezeteinek való szigorú és részletesen szabályozott megfelelést írja elő. Ez a szabályozandó 4 kérdéskör a következő:

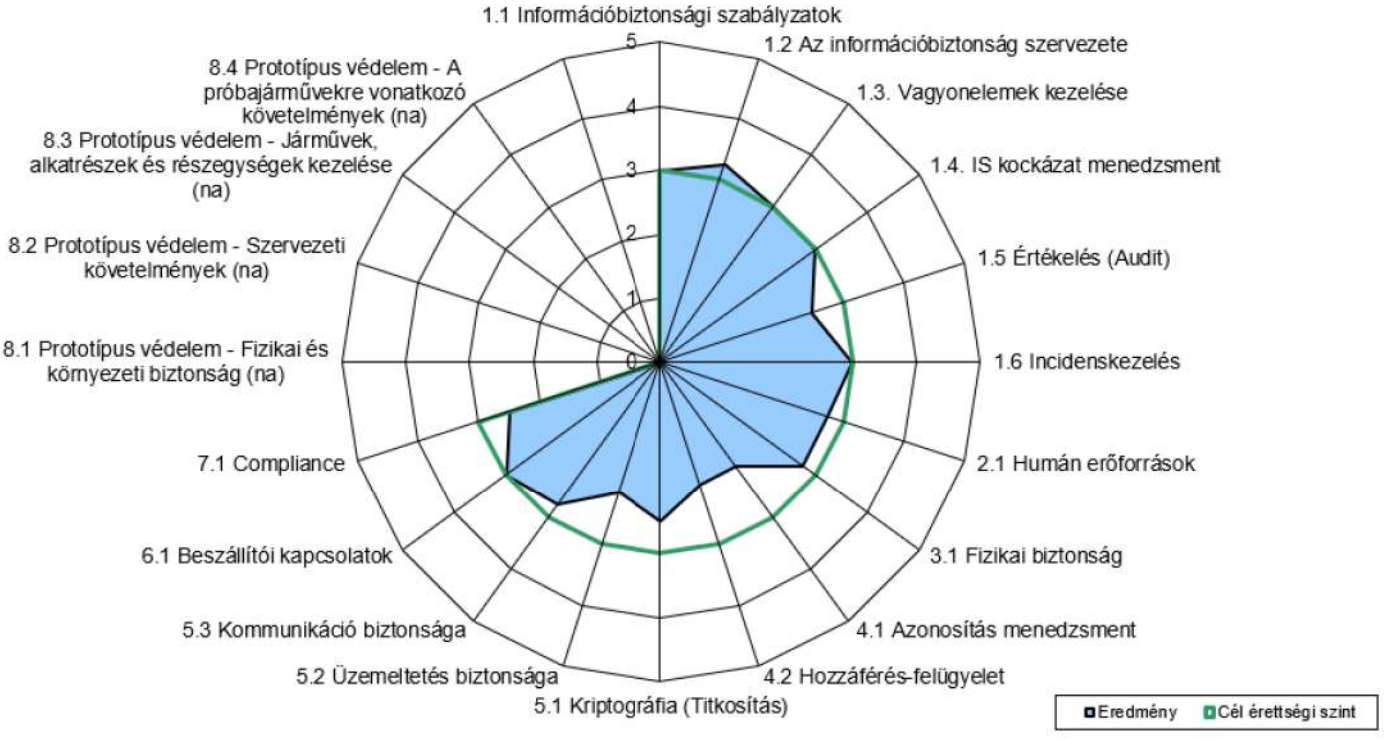
- Milyen mértékben van megszervezve az adatvédelem végrehajtása?

- Milyen mértékben tesznek szervezeti intézkedéseket annak biztosítása érdekében, hogy a személyes adatok feldolgozása a jogszabályoknak megfelelően történjen?
- Milyen mértékben biztosított, hogy a belső folyamatok vagy munkafolyamatok a mindenkori hatályos adatvédelmi előírásoknak megfelelően történnek, és hogy ezeket rendszeresen minőségellenőrzésnek vetik alá?
- Milyen mértékben dokumentálták a vonatkozó adatfeldolgozási eljárásokat az adatvédelmi jog szerinti elfogadhatóságuk tekintetében?

A modul ezekre a kérdéskörökre 24 teljesítendő követelményt határoz meg. A modul teljesítése csak a 7-8. számú TISAX értékelési célok esetén kötelező. (Megjegyzés, hogy a GDPR-nak való alapvető megfelelés már az „Információbiztonság" modulban is megjelenik, ahol a 7.1.2. folyamat önállóan ennek a teljesítését írja elő. Az „Adatvédelem" modul ennek a főfolyamatba beépített további követelményeit tartalmazza, amennyiben az értékelési cél alapján ez külön elvárás.)

A TISAX értékelési Excel táblázat egyben lehetővé teszi egy önálló munkalapon az eredmények szemléletes ábrázolását is. Pókhálódiagram formában láthatóvá teszi az egyes értékelési területek elvárt és teljesített eredményeit. Példaként egy olyan mintavállalat felkészülés közbeni részeredményeinek grafikus ábrázolását mutatjuk be, amelynek csupán az alapnak számító „Információbiztonság" modul teljesítése volt a feladata. Az eredmények ábrázolása a következő 1. sz. ábrán látható.

Az alfejezetekre eső eredmény (csökkentés nélkül):



1. sz. ábra: A TISAX értékelési területek eredményeinek grafikus ábrázolása az ISA alapján

A gyakorlatból látszik, hogy a legtöbb TISAX megfelelési igazolás esetén elégséges az 1. értékelési cél teljesítése, és az AL2 szerinti audit elvégzése. (A COVID miatti különleges helyzet és különleges eljárásmód is sok esetben ezt támogatja.) Ugyanakkor megállapítható, hogy ez a minimumkövetelmény már önmagában is egy részletes és összetett információbiztonsági követelményrendszert takar. Az információbiztonsági szempontoknak és kontrolloknak vonatkozniuk kell a vállalat minden tevékenységére és az azokban lévő biztonságos adatkezelésre. Az információbiztonsági modul kiterjed mind az információbiztonság irányítás szervezeti és technikai követelményeire, mind külön-külön az adminisztratív, a fizikai és a logikai biztonsági kontrollokra.

Ha a másik csoportosítást nézzük, akkor látható, hogy megjelenik az információbiztonság mind az öt szakmai területének az alkalmazása is:

- a fizikai védelmi (őrzés-védelmi) szakma,
- a humán biztonsági szakma,
- a titkos ügyiratkezelési szakma (papír alapú adatok biztonsága),
- az informatikai biztonsági szakma, valamint
- a katasztrófahelyzetek kezelése szakma (információbiztonsági aspektusainak kezelése).

Az információbiztonsági rendszer kialakítása során tehát egyszerre ezeknek a szempontoknak és követelményeknek kell egyidejűleg megfelelni. Ez együtt egy összetett és nagy tapasztalatot és odafigyelést igényló feladat, amit a TISAX-nak megfelelni kívánó vállalatoknak kell megvalósítani tudni.

Összefoglalás

A TISAX egy új, az ISO/IEC 27001-re épülő, de az autóipar sajátosságait és elvárásait erősen figyelembe vevő, így arra testreszabott információbiztonsági követelményrendszert és ahhoz kapcsolódó önértékelési és értékelési rendszert tartalmaz. Amennyiben az autóipari beszállítók – beleértve a beszállítói lánc bármely szintjét – ezt alkalmazzák, és az ENX szisztémája által elfogadott értékelők regisztrált értékelésein (auditjain) megfelelnek, akkor ezeket az értékelési eredményeket az ENX rendszerén keresztül megoszthatják a különböző autóipari megrendelőikkel, amelyek ezt egységesen elfogadják. Noha a TISAX követelményrendszer alapelvárásait (TISAX Résztvevői Kézikönyv, önértékelési ISA csekklista, egyéb hasznos anyagok) az ENX honlapon közzétett dokumentációk mind tartalmazzák, azok értelmezése és gyakorlatba történő hatékony átültetése már sok-sok éves gyakorlatot és információbiztonsági szakmai tapasztalatot igényel.

Látható, hogy a TISAX alapú információbiztonsági rendszer kiépítése összetett és sok szempont együttes összehangolását igénylő feladat. Jellemző, hogy ez nem a vállalati működés melletti, illetve attól független biztonsági szabályzat készítését jelenti, hanem olyan biztonsági szempontok bevezetését, amelyek a mindennapi tevékenységekkel is szoros kapcsolatban vannak. Éppen ezért fontos külön figyelmet szentelni arra, hogy a biztonsági követelmények teljesítése mellett a vállalat a mindennapi tevékenységeinek működését, rugalmasságát és hatékonyságát is megtarthassa. Ezek együttes összhangba hozása sokszor már nagy tapasztalatot igénylő feladat, aminek megvalósítására szükséges rászánni a kellő erőforrásokat.

Felhasznált Források

[1] AUDI HUNGARIA Zrt. Általános Információtechnológiai Feltételek – 2021.07.29. napjától hatályos változat, https://audi.hu/hu/letoltesek/beszerzes/123 (letöltés: 2022.01.08.)

[2] Dr. Horváth Zsolt: TISAX, az autóipar új információbiztonsági követelményrendszere, Magyar Minőség 2020. június

[3] TISAX Participant Handbook, Version 2.3., 1.20.2021, https://portal.enx.com/tphen.pdf (letöltés: 2022.01.08.)

[4] Information Security Assessment (ISA), Version 5.0.4., 1.20.2021, https://portal.enx.com/isa5-en.xlsx (letöltés: 2022.01.08.)

Dr. Horváth Zsolt az INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft. tulajdonosa és ügyvezetője 2006 óta. EOQ MNB által regisztrált minőségirányítási és információbiztonsági rendszermenedzser és auditor. Tíz évig látta el a SIEMENS magyarországi szoftverházának, a SIEMENS PSE Kft-nek a minőségirányítási igazgatói feladatait. Több, mint húsz éve dolgozik a minőségirányítás és az információbiztonsági irányítás területén, több akkreditált tanúsító szervezet vezető auditoraként, valamint tanácsadóként és szakmai oktatóként. Számos szakmai konferencián elhangzott előadás és megjelent publikáció szerzője és társszerzője.

A Menlo Parki varázsló

Sokak véleménye szerint a 175. évvel ezelőtt, 1847. február 11-én született **Thomas Alva Edison** minden idők legnagyobb feltalálója volt. Ohio államban született, szüleinek legfiatalabb, hetedik gyermekeként. Iskolába gyakorlatilag nem járt, tanítónő édesanyja tanította írni, olvasni és számolni. Érdeklődő gyerek volt, búvta a könyveket, imádott olvasni.

13 évesen már a vasúton „utasellátóként" dolgozott, a heti 50$ keresetét kísérleti anyagokra költötte. Itt tanulta ki a távírász szakmát is. Első üzleti sikere is ehhez kötődik, az egyszerre 4 üzenetet tudott küldeni. A jogdíjból építette meg a New Jersey-ben a Menlo Parki laboratóriumot, amely a világ első kutató laboratóriuma lett, itt születtek korszakos találmányai. Az Egyesült Államokban 1093, az egész világon 2332 szabadalmat jegyeztetett be. Ezek közvetlenül hasznosítható elektromos, mechanikai vagy kémiai jellegű eszközökre vagy folyamatokra irányultak, fonográf, izzólámpa és még mások.

Persze, nem volt tévedhetetlen, az áramellátásban Tesla-nak lett igaza.

Cukorbetegségére nem talált megoldást, 1931 október 18-án hunyt el.