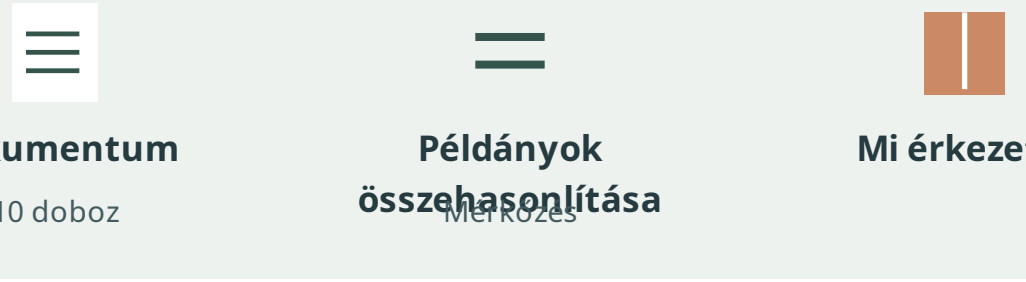
Az ötlet

Amit tudunk, hogyan lehet ellenőrizni, és amit még nem tudunk

A Konfirmu útmutató családok, tanárok, döntéshozók és szakemberek számára.



Két dokumentum szerint tíz doboz érkezett. Valaki elmegy a raktárba, megszámolja a padlón lévő dobozokat, és kilencet talál.

Ellenőrizhetjük, hogy a dokumentumok egyeznek-e. Ahhoz, hogy megtudjuk, hány doboz érkezett, szükségünk van a darabszámra is. Milyen igazolást kérnél az átvevő személytől?

A bizonyítékok három szintje

Mit tudunk ellenőrizni?

A másolat, az aláírás és a számlálás különböző kérdésekre ad választ.

01 Van valami megbízható forrásunk?

Ez lehet maga az eredeti fájl, vagy annak digitális ujjlenyomata, amelyet megbízható csatornán keresztül szereztek be. A hivatkozás verzióját és forrását is őrizzék meg.

02 A másolat ugyanazokat az adatokat tartalmazza?

A hash egy fájl bájtjaiból kiszámított digitális ujjlenyomat. A digitális aláírás megbízható kulccsal történő ellenőrzése lehetővé teszi az aláíró kulcsához fűződő kapcsolat igazolását is.

03 A dokumentumban szereplő esemény valóban megtörtént?

Ahhoz, hogy kiderüljön, mi történt, előfordulhat, hogy meg kell számolnia a dobozokat, ellenőriznie kell egy mérést, át kell néznie egy hivatalos nyilvántartást, vagy meg kell kérnie egy szakértőt, hogy vizsgálja meg a bizonyítékokat.

Három lehetséges válasz

„Egyezik”, ha a másolatok megegyeznek. „Különbözik”, ha eltérnek egymástól. „Még nem tudom”, ha hiányzik egy hivatkozás vagy más bizonyíték.

Offline módban ellenőrizheti, hogy a készülékén már rendelkezésre állnak-e az adatok, a hivatkozás és az eszközök. Az elveszett eredeti példányt csak akkor állíthatja vissza, ha létezik róla másolat.

A hibák, amelyeket megtanultunk felismerni

A november 25-i tudományos feljegyzésből származó hat megállapítás. Minden vizsgálati eredmény a feljegyzésben megjelölt verzióra vonatkozik.

F1 A 95%-os határérték kevesebbet is lefedhet

Amit megállapítottunk

Ebben a példában a lineáris módszerrel kiszámított felső határ az értékek 86,51%-át fedi le, bár névleges szintje 95%.

Hogyan lehet ellenőrizni

A 7. oldalon bemutatjuk, hogyan kell kiszámítani a lefedettséget egy olyan normális eloszlású változó reciprokjára, amelynek átlaga 1, szórása pedig 0,3.

Amit ez nem bizonyít

Az eredmény erre a modellre és ezekre a határértékekre vonatkozik. Más mérések esetén új számítást kell végezni.

Az F1-et ebben a kiadásban újraszámolták. A csapat november 24-én is elvégezte a számítást.

F2 A nyugta és az adag mérete

Amit megállapítottunk

Egyes tételek esetében a vizsgált verzió által kiállított nyugta nem tudta megerősíteni, hogy hány darab volt jelen.

Hogyan lehet ellenőrizni

Az ellenőrzés során rögzíteni kell, hogy hány tétel érkezett be, és milyen bizonyítékok támasztják alá, hogy ez a mennyiség egyezik a nyugtán szereplővel.

Amit ez nem bizonyít

Ez korlátozza, hogy a nyugta milyen információkat tartalmaz az adott tételről. A jelentés szerint az SHA-256-ban nem történt megszakítás.

A csapat november 24-én megismételte az F2 hibát. A jegyzetben ezt a problémát a 3.0.0-s verzióban nyitottként rögzítették.

F3 Amikor az adatok közötti különbség eltűnik

Amit megállapítottunk

A tárolt ábrázolásból hiányzott egy, a forrásadatokban még meglévő megkülönböztetés. A nyugta már nem tudta ezt igazolni.

Hogyan lehet ellenőrizni

Az áttekintés során a csapatnak képesnek kell lennie arra, hogy bizonyítsa: a dokumentum az eredeti minden lényeges megkülönböztetést megőriz.

Amit ez nem bizonyít

Az adatok ábrázolásakor ez a különbség eltűnt. A teszt nem bizonyít kriptográfiai ütközést.

A csapat november 24-én megismételte az F3 hibát. A jegyzetben ezt a problémát a 3.0.0-s verzióban nyitottként rögzítették.

Mikor kell a rendszernek leállnia

A november 25-i tudományos feljegyzésből származó hat megállapítás. Minden vizsgálati eredmény a feljegyzésben megjelölt verzióra vonatkozik.

F4 Két ellenőr eltérő választ adott

Amit megállapítottunk	Hogyan lehet ellenőrizni	Amit ez nem bizonyít
A belső felülvizsgálati jelentés szerint az egyik ellenőr a 9 módosításból 7-et észlelt, a másik pedig mind a 9-et.	Egy új verzió értékeléséhez hasonlítsa össze annak döntéseit a várt döntésekkel, és őrizze meg a tesztelési eredményeket.	Kilenc példa alapján nem lehet megállapítani, hogy egy másik dokumentumkészletben hány változást lehetne észlelni.

Az F4-es hibáról a november 24-i belső felülvizsgálat során számoltak be. A csapat nem hajtotta végre újra a tesztet a jegyzet kedvéért.

F5 „OK” jelzés, amikor a szabály szerint meg kellett volna állni

Amit megállapítottunk	Hogyan lehet ellenőrizni	Amit ez nem bizonyít
A csapat négy olyan helyzetet azonosított, amelyekben a válasz „OK” volt, noha a szabály szerint „VETO”-t kellett volna adni.	A javasolt javítás hatására az 1 246 teszteset közül 186 nem adta többé az „OK” eredményt. Egyik sem vált „OK”-ra.	A jegyzet egy javasolt javítást ismertetett. Az éles környezetben való alkalmazásának jóváhagyásához szükség van a telepített verzióra vonatkozó bizonyítékra és a hozzá tartozó tesztekre.

Az F5-ről november 24-én érkezett bejelentés. November 25-én a jegyzetben rögzítették, hogy a javítás még nem került nyilvánosságra.

F6 A mérési érték nagyon közel van a határértékhez

Amit megállapítottunk	Hogyan lehet ellenőrizni	Amit ez nem bizonyít
Egy olyan példában, ahol a határértékek 2 és 8 voltak, a mért érték hat tizedesjegyre történő kerekítése eltérő eredményt adott, mint a nagyobb pontosságú kerekítés.	Az ellenőrzésnek meg kell határoznia az alkalmazott pontosságot és a mérési eredmény és a határérték összehasonlítására vonatkozóan elfogadott szabályt.	A tűréshatár a felhasználás céljától és az alkalmazandó szabálytól függ. Ez a példa más felhasználási esetekre nem határoz meg tűréshatárokat.

Az F6-ról november 24-én érkezett bejelentés. A jegyzet megírásakor a vonatkozó szabály még tárgyalás alatt állt.

Egészség és orvostudomány

Egészségügyi dokumentum ellenőrzése

Három kitalált helyzet, amelyekben valaki összehasonlíthat egy adatot egy megbízható referenciaértékkel.

01 Oltási könyv

Egy összehasonlításból kiderülhet, hogy egy példányt módosítottak. Az oltás beadásának megállapításához a klinikai vizsgálatból származó bizonyítékra van szükség. A hatékonyság igazolásához külön bizonyítékra van szükség.

02 Egy laboreredmény

Ellenőrizheti, hogy a kapott jelentés egyezik-e a laboratórium által rögzített jelentéssel. A tényleges eredményt egészségügyi szakembernek kell értelmeznie.

03 Hűtési lánc nyilvántartás

Összehasonlíthatja a napló másolatát a referenciaadatokkal. Az érzékelő kalibrálását és a tényleges tárolási körülményeket külön-külön kell ellenőrizni.

Előfordulhat, hogy egy érzékelő helytelen értéket rögzít

Tegyük fel, hogy egy érzékelő 4 °C-ot jelez. Ha az érzékelő meghibásodott, a tényleges hőmérséklet eltérhet attól, még akkor is, ha a másolat megegyezik az eredeti naplóval.

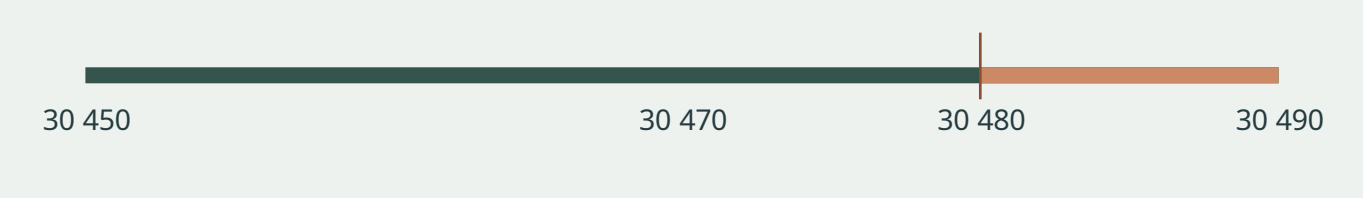
A tudományos ismertető a Konfirmu-t kutatási prototípusként írja le. Nem orvostechnikai eszköz, és nem diagnosztikai, kezelési vagy egyénekre vonatkozó döntéshozatali célokra tervezték.

Működési biztonság és szavazás

Egy érvényes nyugta tartalmazhatja a „stop” szót

Laboratóriumi teszt egy fiktív tartály felhasználásával és egy hipotetikus 30 480 kg-os határértékkel.

A mérlegelt tömeg: 30 470 ± 20 kg



Súlytartomány, kilogrammban · határ 30 480 kg
https://dpsindustrial.nl/konfirmu/guia/pesagem/?lang=hu

A tartomány 30 450 és 30 490 kg között mozog. A határérték és a súly különbségeként számított tűréshatár −10 és +30 kg között mozog. A tartomány felső határán a súly 10 kg-mal meghaladja a határértéket. Az átvételi elismervényen érvényes aláírás (VALID) szerepelhet, miközben a szabály szerint leállítást (VETO) kellene alkalmazni.

Mi a helyzet a szavazással?

Az aláírt jegyzőkönyv ellenőrzése feltárhatja a későbbi módosításokat. A választók hozzáférésének biztosítása, a szavazatszámlálás pontossága és a szavazás titkossága mindegyike saját bizonyítékot igényel. Az a nyugta, amelyből kiderül egy személy választása, veszélyeztetheti a titkosságot.

Ki jogosult engedélyezni a műveletet?

Az aláírás segítségével ellenőrizni lehet a dokumentumot. A felelős személyek a tényleges műveletre vonatkozó szabályok és adatok alapján döntik el, hogy folytatják-e a folyamatot.

Ellenőrzések a készüléken

Hogyan ellenőrizheted magad?

Egy megbízható referencia segítségével összehasonlíthat egy fájlt. Emellett megismételheti a 3. oldalon szereplő lefedettségi számítást is.

A megjegyzés a Python motor 3.0.0-s verzióját jelöli meg, a 90b3968-as commit-számmal, 2026. november 24-i dátummal. A kód az EUPL-1.2 licenc alapján áll rendelkezésre.

Hivatalos kódtár

A Python-motor SHA-256-ja, amint az a megjegyzésben szerepel
`529098c652ee8234960d69383e308f60db6a5df8ea6bdae578b538eb806e80cf`

Helyezze a kiadási manifesztet és a hozzá tartozó fájlokat egy mappába. Futtassa a rendszeréhez megfelelő parancsot.

```
sha256sum -c SHA256SUMS.txt        # Linux
shasum -a 256 -c SHA256SUMS.txt    # macOS
```

A csapat 62 egyező fájlt, 247 önellenőrzést és 10 szabálykészletet jelentett, amelyeket Linux rendszeren, Python 3.13-mal teszteltek. Ezek az adatok az említett áttekintéshez tartoznak.

F1 · Ismételje meg a számítást Pythonban

```
from statistics import NormalDist
X, Z = NormalDist(1, 0.3), NormalDist()
u = 1 + Z.inv_cdf(.95) * .3
print(u, X.cdf(0) + 1 - X.cdf(1/u))
print(X.cdf(1/.412) - X.cdf(1/1.588))
```

Y = 1/X esetén a felső határ 1,493456088, a lefedettség pedig 86,51%. A negatív X-értékek is megfelelnek ennek a határértéknek. A közzétett, kerekített kétoldali határértékek (0,412 és 1,588) 89,14%-os lefedettséget eredményeznek.

A lefedettség ebben a modellben a valószínűséget jelenti. A jegyzet a bizonytalanság terjedésével kapcsolatban a JCGM 100 és 101 számú dokumentumokra hivatkozik.

Nyisd meg a böngészőalkalmazást · 143 662 B

https://dpsindustrial.nl/konfirmu/app/

Nyissa meg a „Fájlok összehasonlítása” menüpontot. Válassza ki a referenciafájlt és a második példányt, majd válassza az „A4 · Összehasonlítás” lehetőséget.

Compare files → Reference file → Second copy → A4 · Compare

A böngészőalkalmazás HTML-fájljának SHA-256-értéke, ellenőrzés dátuma: 2026. november 26.
`0a468ec23401f5125ee1e5399ef536b6fba88beab94771e4df6b7910c9723717`

Korlátok és további vizsgálatok

Amit még mindig nem tudunk

Bárki, aki bizonyítékot kap, ellenőrizheti azt. Hogy mit támaszt alá a bizonyíték, az a hivatkozástól és az alkalmazott vizsgálati módszertől függ.

Ki végezte el a vizsgálatokat?

A november 25-i feljegyzés a teszteket a csapatnak és az általa használt mesterséges intelligencia-rendszereknek tulajdonítja. Egy független vizsgálat azonosítaná a verziót, megismételné a teszteket, és rögzítené az eredményeket, beleértve az eltéréseket is.

Milyen elismerésről van szó?

Az ECSS-Q-ST-80C Rev.2 szabvány 295 követelményeinek megfelelő ellenőrzés önértékelés formájában történt. Az i-DEPOT 162925 és 164391 számú bejegyzései rögzítik, hogy mit és mikor rögzítettek. A termékminőséget külön értékelés keretében kell vizsgálni.

Mit lehet egy időbélyeggel megállapítani?

A Chronolex lehetővé teszi az olvasók számára, hogy ellenőrizzék a feljegyzések hitelességét. A megjegyzés szerint a használt ingyenes, nyilvános időbélyegző-szolgáltatás nem biztosít garantált jogi hatályt. Továbbra is szükség van az esemény bekövetkeztét igazoló bizonyítékra.

Eltérést találtál?

Jegyezze fel a verziót, a várt eredményt és azt, amit észrevett. Küldje el a részleteket a következő címre:

admin@dpsindustrial.nl

Olvassa be vagy érintse meg a megnyitáshoz

A DPS hivatalos honlapja

12 szektoros készlet

A ZIP-fájlban nyissa meg az Exemplos/09-Shipping/ mappát. Hasonlítsa össze az alkalmazásban található 01-original.txt és 02-copia.txt fájlokat: a fiktív rekordok 24, illetve 29 dobozt jelölnek. A mérési példa a 6. oldalon található.

Elsődleges forrás · Tudományos megjegyzés, 2026. november 25.
Konfirmu_Scientific_Note.pdf · 88 212 B · SHA-256
884fde70000fa68dccdb4b6527da7a1bce8a7737b3f44c03340f182ae6100f88
DPS Industrial & Maritime Services · Konfirmu · KVK 42005886
Enschede, Hollandia