iskraemeco
BY ELSEWEDY ELECTRIC

Kibernetska varnost, se zavedamo nevarnosti in posledic?

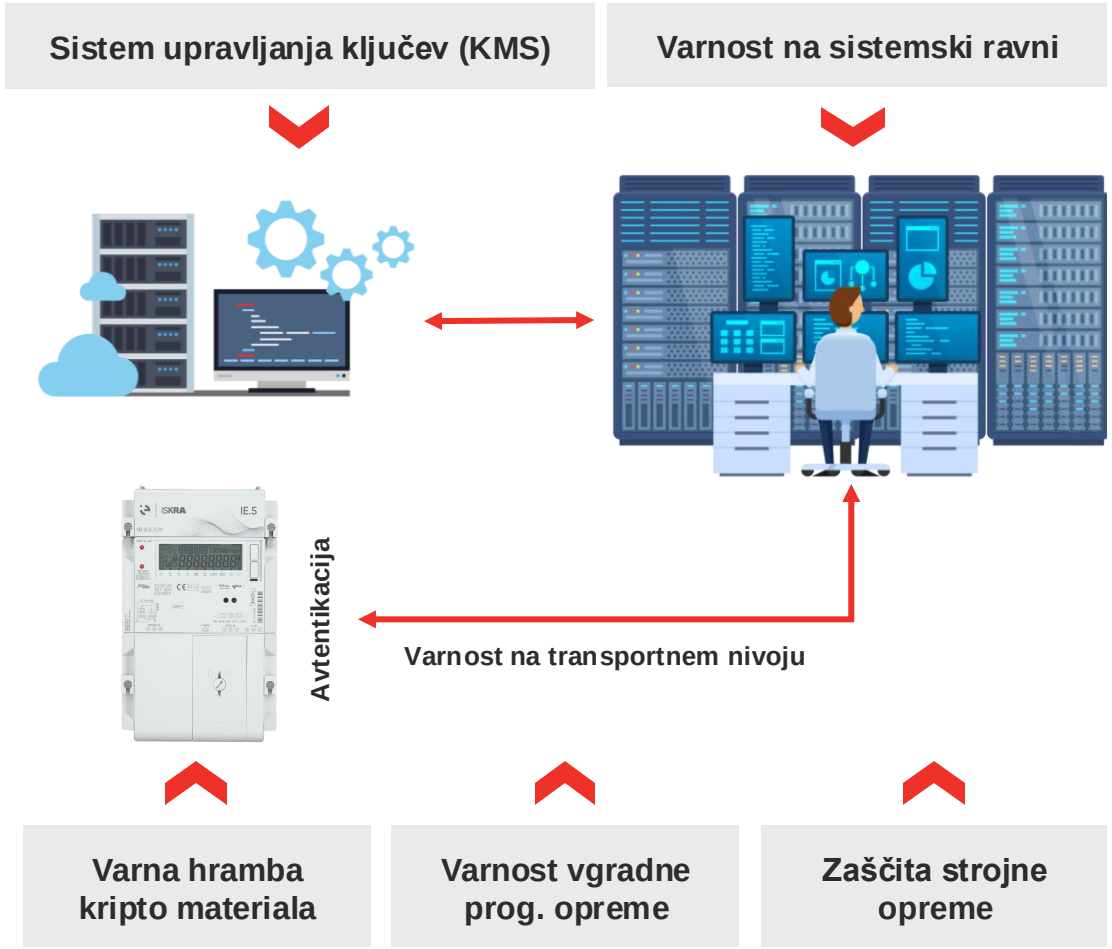
Dr. Simon Oblak,
Globalni direktor za upravljanje rešitev

Varnostni izzivi pametnih omrežij

- **Napadi na merilne naprave**: Fizični dostop do merilnih naprav lahko omogoči dostop do kritičnih podatkov, manipulacijo s podatki ali celo onesposobitev sistema.
- **Napadi na komunikacijsko omrežje**: Komunikacijski kanali med merilnimi napravami in centralnim sistemom so lahko tarča napadov, kot so zlonamerni vložki, prisluškovanje ali zavajanje.
- **Napadi na centralni sistem**: Centralni sistem, ki obdeluje in shranjuje podatke, mora biti zaščiten pred vdori, zlonamernimi programi in drugimi grožnjami, ter dovolj skalabilen za nemoteno delovanje.
- **Napadi na programsko opremo**: Napadi na vgradno programsko opremo (FW) lahko omogočijo spreminjanje ključnih funkcij, onemogočijo varnostne mehanizme in ogrozijo delovanje sistema (npr. masovni odklop porabnikov).
- **Nadzor dostopa**: s politiko avtorizacije je potrebno preprečiti dostop do elementov / funkcij sistema nepooblaščenim osebam.
- **Zasebnost**: Zaščita zasebnosti končnih odjemalcev je ključna zaradi obdelovanja občutljivih podatkov.

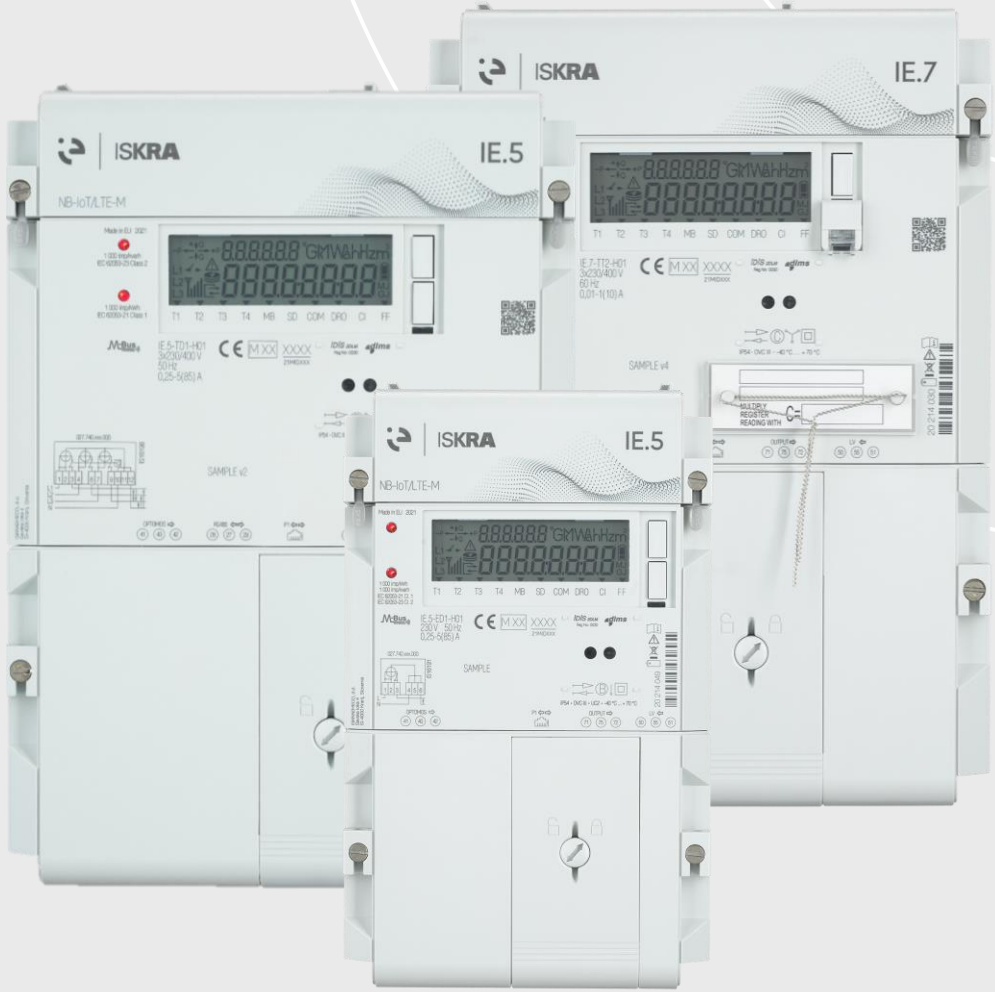
Koncept varnosti na celotni poti izmenjave informacij (E2E security)

- **Zaščita pred vdorom na napravah**
- **Avtentikacija in zaupnost** -> visoka raven varnosti (HLS) in nadzor dostopa na podlagi vlog (RBAC)
- **Zaščita pred napadi** na transportnem in aplikacijskem nivoju
- Delitev sistema na **varnostne cone**
- **Ščitenje dostopa do sistema** (https, TLS)
- **Ločen sistem KMS**
- **Varno ravnanje s ključi** (generiranje, prenos, namestitev, menjava)
- **Večnivojsko logiranje** na vseh komponentah



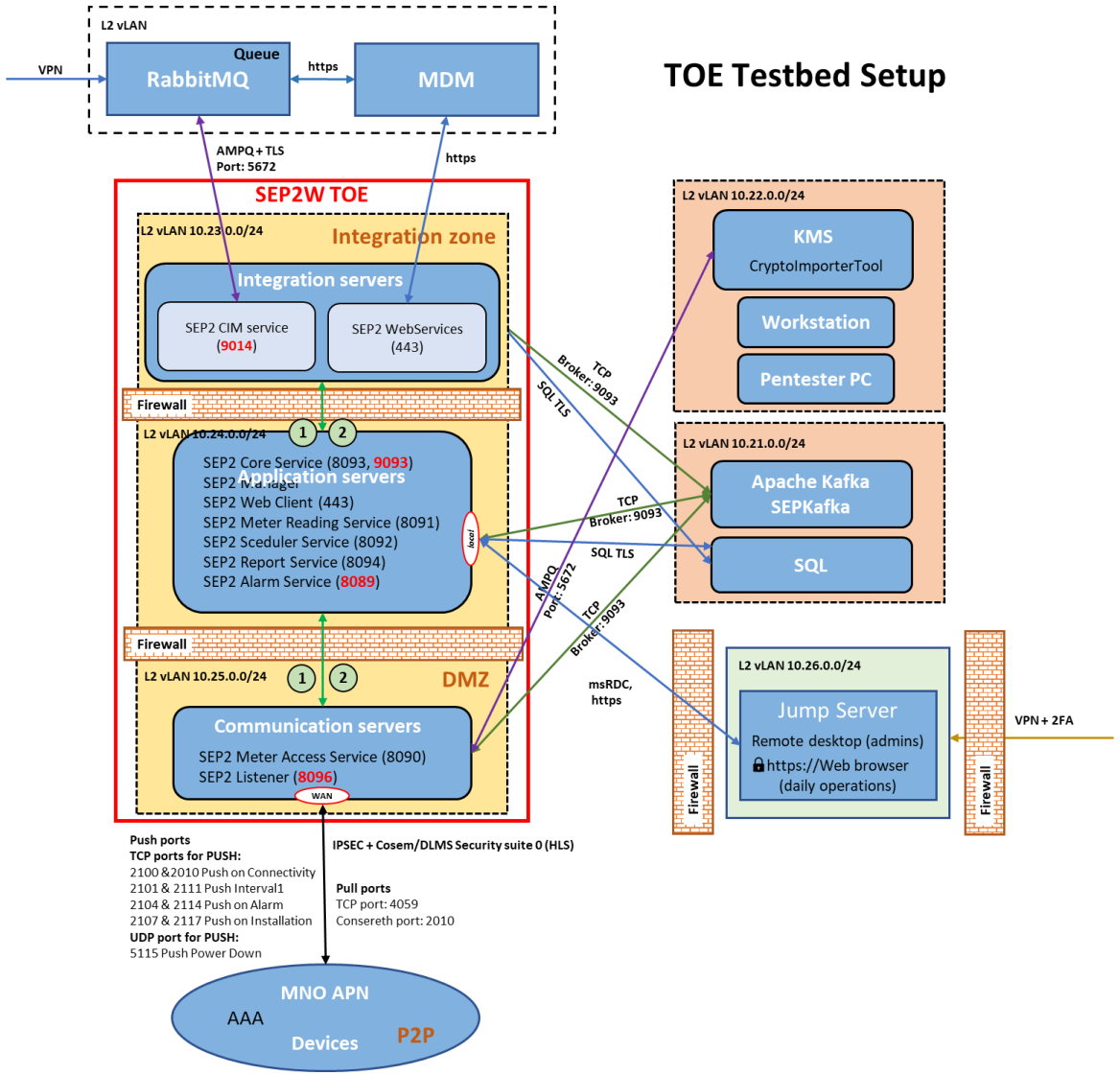
Varnost na pametnih števcih

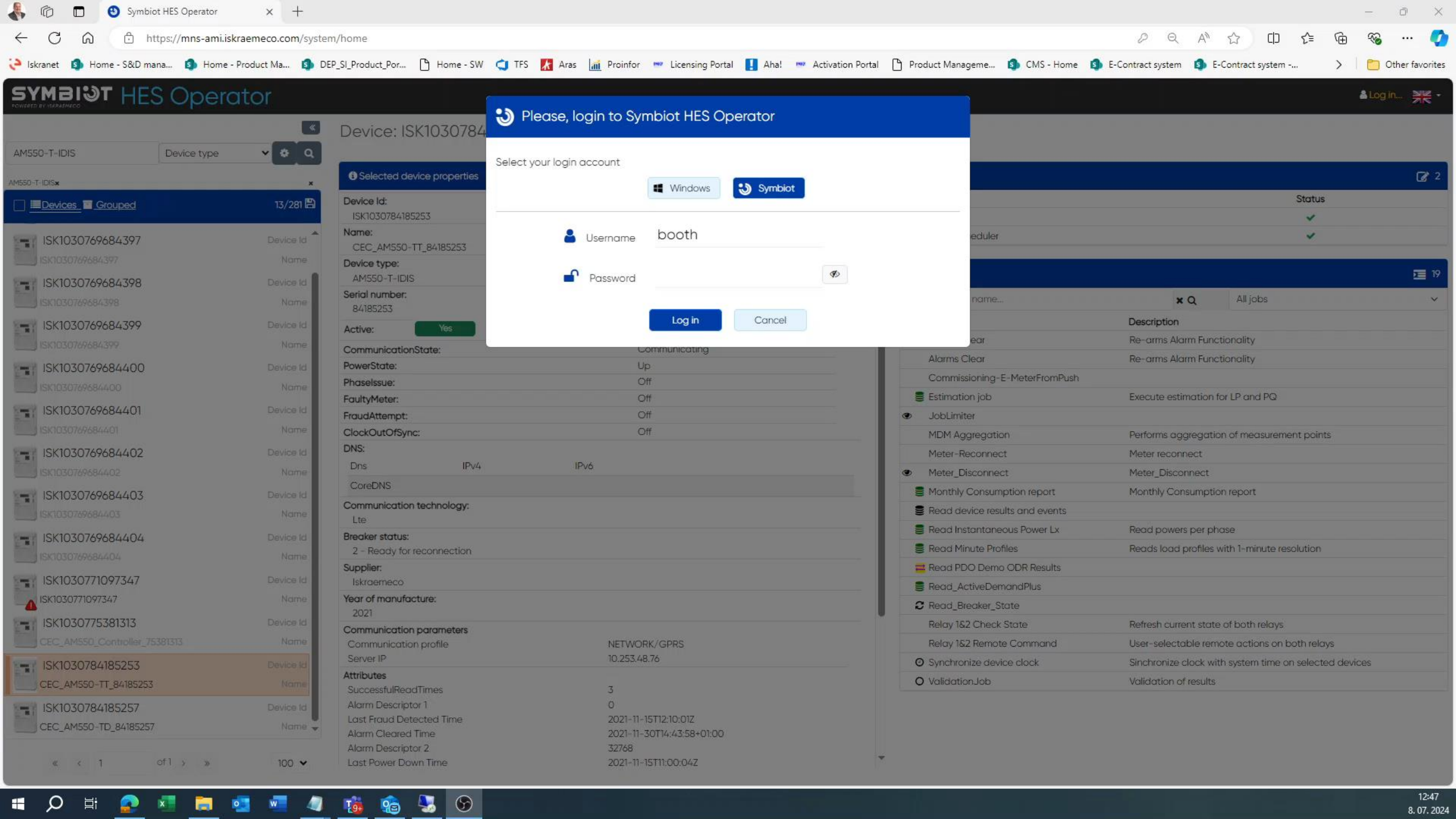
- **Detekcija fizičnega vdora** (pokrovi, magnet, …)
- **Visoka raven varnosti COSEM / DLMS** na vseh vmesnikih
  - Avtentikacija klienta po HLS GMAC
  - Nadzor dostopa na podlagi vlog (RBAC)
  - E2E kriptiranje podatkovnih transakcij
  - Varna hramba in izmenjava kriptografskega materiala
- **Mehanizmi za zaščito pred napadi na transportnem in aplikacijskem nivoju** (replay attack, blokada avtentikacije, …)
- **Zaščita pred vdori in spremembami podatkov** ali vgradne programske opreme (FW)
- **Namenski dnevnik** za varnostne dogodke (security log)



Varnost na sistemu HES

- **Visoka raven varnosti COSEM / DLMS proti števcem**
  - HLS GMAC avtentikacija in E2E kriptiranje podatkovnih transakcij
  - Varna hramba in izmenjava kriptografskega materiala
- **Interni ali eksterni KMS po KMIP 1.4** (brez izpostavljanja ključev)
- **Varovanje internih povezav** (TLS, https, …)
- **Večnivojsko logiranje dogodkov** (security, audit)
- **Varnostna politika dostopov** (security policy & user rights, access policy & rights)
- **Aktivno omejevanje izvajanja kritičnih operacij**
  - Dodatna avtorizacija (4-eye principle)
  - Limitacija frekvence izvajanja




Symbiot HES Operator
https://mns-ami.iskraemeco.com/system/home
SYMBIOT HES Operator
Please, login to Symbiot HES Operator
Select your login account
Windows
Symbiot
Username
booth
Password
Log in
Cancel
Device: ISK1030784
Selected device properties
Device Id: ISK1030784185253
Name: CEC_AM550-TT_84185253
Device type: AM550-T-IDIS
Serial number: 84185253
Active: Yes
CommunicationState: Communicating
PowerState: Up
PhaseIssue: Off
FaultyMeter: Off
FraudAttempt: Off
ClockOutOfSync: Off
DNS:
Dns IPv4 IPv6
CoreDNS
Communication technology: Lte
Breaker status: 2 - Ready for reconnection
Supplier: Iskraemeco
Year of manufacture: 2021
Communication parameters
Communication profile NETWORK/GPRS
Server IP 10.253.48.76
Attributes
SuccessfulReadTimes 3
Alarm Descriptor 1 0
Last Fraud Detected Time 2021-11-15T12:10:01Z
Alarm Cleared Time 2021-11-30T14:43:58+01:00
Alarm Descriptor 2 32768
Last Power Down Time 2021-11-15T11:00:04Z
Status
Description
Re-arms Alarm Functionality
Alarms Clear
Re-arms Alarm Functionality
Commissioning-E-MeterFromPush
Estimation job
Execute estimation for LP and PQ
JobLimiter
MDM Aggregation
Performs aggregation of measurement points
Meter-Reconnect
Meter reconnect
Meter_Disconnect
Meter_Disconnect
Monthly Consumption report
Monthly Consumption report
Read device results and events
Read Instantaneous Power Lx
Read powers per phase
Read Minute Profiles
Reads load profiles with 1-minute resolution
Read PDO Demo ODR Results
Read_ActiveDemandPlus
Read_Breaker_State
Relay 1&2 Check State
Refresh current state of both relays
Relay 1&2 Remote Command
User-selectable remote actions on both relays
Synchronize device clock
Sinchronize clock with system time on selected devices
ValidationJob
Validation of results
ISK1030769684397
ISK1030769684398
ISK1030769684399
ISK1030769684400
ISK1030769684401
ISK1030769684402
ISK1030769684403
ISK1030769684404
ISK1030771097347
ISK1030775381313
ISK1030784185253
CEC_AM550-TT_84185253
ISK1030784185257
CEC_AM550-TD_84185257
12:47
8. 07. 2024

Certifikacija komponent

- **Redno testiranje varnostnih mehanizmov in certificiranje s strani neodvisnih ustanov**
- **Pametni merilniki**
  - Riscure ocena ranljivosti (vulnerability review)
  - Brightside ocena varnosti (security assessment)
  - CCLab Metas Data Security certifikat
  - DLMS (varnostni paket COSEM / DLMS)
  - LANpark (varnost na G3-PLC)
  - statična analiza za Security CVE v procesu razvoja (SonarQube)
- **HES**
  - CENELEC 2016
  - ISO 27001 / 27017 / 27018 / 33061
  - CCLab Metas Data Security certifikat

ISO 9001:2015

From SGS

From SIQ

From IQNet

ISO 14001:2015

From SGS

ISO 45001:2018

From SGS

ISO 17025:2017

From EGAC

ISO 27001:2013:

From BV

MID 2014/32/EU

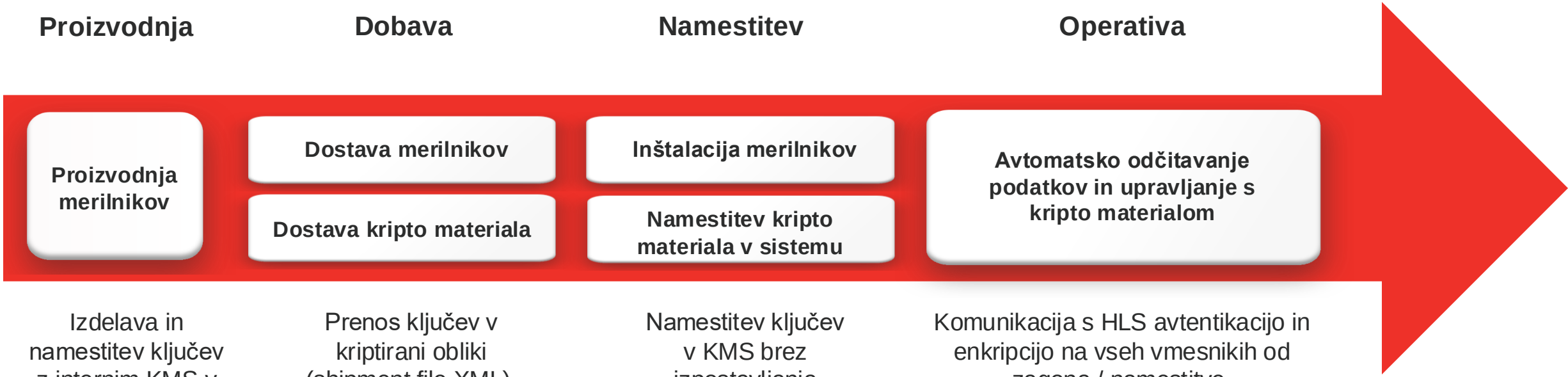
From MIRS

From SIQ

PTB approval

IRAM Approval

Varnost pri ravnanju s kriptografskim materialom



Izdelava in namestitev ključev z internim KMS v proizvodnji.

Prenos ključev v kriptirani obliki (shipment file XML).

Namestitev ključev v KMS brez izpostavljanja vsebine

Komunikacija s HLS avtentikacijo in enkripcijo na vseh vmesnikih od zagona / namestitve.

Avtomatizirana menjava kripto materiala s pomočjo KMS.

Nadzorovan dostop do sistemskih funkcij v povezavi z varnostjo.

Kaj prihaja?

Paket COSEM / DLMS varnostni paket 1 (Security Suite 1)

- Digitalno podpisovanje kritičnih operacij
- Preverjanje identitete podpisnika
- Kompresija podatkov
- Uvedba PKI infrastrukture

Certifikacija števcev PSA Certified

- V pripravi certifikacija po PSA nivoju 1 (Riscure)
- Razširitev na nivo 2 in 3
- Priprava na EU akt o kibernetski odpornosti (CRA)

Edge moduli z varno povezljivostjo v oblak

- Vzpostavljanje individualnih VPN tunelov
- Detekcija kibernetskih napadov neposredno na merilnikih

iskraemeco
BY ELSEWEDY ELECTRIC

Hvala za pozornost!

www.iskraemeco.com