Technická specifikace: Zadávací podmínky na SW a HW platformu CŘE

1. Funkční požadavky

1.1. Uživatelská aplikační vrstva (frontend)

Aplikace musí být přístupná z běžně používaných webových prohlížečů bez nutnosti instalace (např. Microsoft Edge, Google Chrome, Safari, Opera, Seznam a podobně) umožňující dohled, dispečink, monitoring a vzdálené řízení spotřeb a zdrojů nezávislé na výrobci instalovaných HW prvcích jednotlivých měřících a řídích prvků. Přes toto rozhraní probíhá kompletní správa a parametrizace systému.

1.2. Serverová část (backend)

Serverová část aplikace může být dodána jako služba formou pronájmu (SaaS), nebo jako nákup dedikované verze (pořízení trvalých licencí). Serverová dedikovaná verze aplikace musí být schopna běhu v prostředí MS Windows i Linux. Služba pronájmem musí prokazatelně splňovat platné podmínky serverových služeb minimálně TIER3 a kybernetické bezpečnosti (NIS1) a být plně připravena na nově připravované podmínky (NIS2).

1.3. Řízení účtů a uživatelských přístupů

Systém řídí přístupy uživatelů na základě přidělených práv a přístupů k lokalitám nebo jiným způsobem tak, aby bylo vždy zřejmé, kdo danou lokalitu, zdroj nebo spotřebič monitoruje, řídí nebo za něj odpovídá. Řízení uživatelů má jasnou strukturu a obsah.

1.4. Řízení výkonu a spotřeby přes aplikační rozhraní (API)

Systém musí být schopen přes API rozhraní řídit výkony jednotlivých zdrojů a být schopen předávat řídící povely pro řízení spotřeb v řízených lokalitách. Toto API musí být otevřené a být popsáno v manuálu takovým způsobem, aby jeho implementaci mohly dělat externí firmy realizující MaR zdroje nebo spotřeby v dané lokalitě např. kotelně. A to včetně řízení výkonu a spotřeby na základě agregace a flexibility. Řízení může probíhat jak ručně, tak automaticky. API rozhraní musí umožnit co nejjemnější periodu řízení, nejméně však co 2 vteřiny. Řízení lokalit probíhá v zálohovaném i online režimu. Řízení musí být spojeno s predikcí a vyhodnocovat a navrhovat scény a postupy co nejefektivněji.

1.5. Kompatibilita s ISO

Systém je plně kompatibilní se systéme ISO-50001, eviduje a poskytuje data dle tohoto systému. Systém musí plně podpořit certifikace organizace dle tohoto ISO-50001

1.6. Monitorovaná a řízená data

Systém umí monitorovat a sledovat jakékoliv fyzikální a chemické veličiny, které lze senzoricky měřit a převést na číslo interpretující hodnotu nebo stav této veličiny. Může se např. jednat o elektrickou veličinu, plyn, vodu, koncentraci látek, teplotu, stav jištění atp.

1.7. Získávání dat

Systém musí být schopen přijímat data zcela automaticky z velkého množství monitorovaných stanovišť alespoň každých pět sekund. Monitorované lokality mohou odesílat velké množství dat o teplotách, spotřebě, výrobě, ventilech, jištění a další hodnoty. Systém musí být tato velká data schopen přijmout dle první věty tohoto odstavce a zpracovat. Perioda ukládání hodnoty veličiny musí být nastavitelná.

Systém musí být taktéž schopen přijmout a zpracovat ručně zadávaná data. Vstupní data pořizují uživatelé systému s právy zadat konkrétní veličiny.

Hodnoty musí obsahovat informaci kde přesně vznikly (např. automaticky v určité lokality, zadané definovaným uživatelem, vypočtené systémem)

Systém je schopen importovat data ze souborů s běžnou strukturou typu XML, XLS případně dalších. Taktéž musí být schopen importovat data o PENB z XML.

Data zadávaná uživatelem musí mít interní kontrolu definovaných odchylek změn, např. když jeden měsíc zadá spotřebu 100 kWh a druhý měsíc 10 kWh, musí se systém zeptat na správnost zadaných dat (princip poka-yoke). Tyto odchylky musí být nastavitelné, např procenty, velikostí změny apod.

1.8. Ukládání a správa souborů

Je nutné mít možnost uchovávat soubory k jakékoliv položce struktury lokalit a měřidel. Budou se zde uchovávat zejména, nikoliv však výlučně, PENB, certifikáty měřidel, revizní zprávy a podobné dokumenty.

1.9. Napojení na GIS

Systém bude přes API rozhraní poskytovat data systému GIS pro online vizualizaci na mapových podkladech.

1.10. Možnost integrace zdrojů a bateriových úložišť

Platforma musí umožnit propojení s jakýmkoliv zdrojem i bateriovým úložištěm jiného dodavatele nebo výrobce v budoucnu pro lokální automatické řízení bilance. Propojení musí být zajištěno průmyslovým komunikačním protokolem bez nutnosti licenčních poplatků. Zdrojem je myšlen nejen zdroj elektřiny, ale i plynu, vody, tepla, výrobna vodíku, dieselagregát, kogenerační jednotka, kotelna atp. Spotřebou je jakýkoliv spotřebič, vzduchotechnika, bojlery, kotelna, osvětlení, kompresory, tepelná čerpadla, nabíječky atp.

1.11. Integrace nabíjecích stanic elektromobility

Systém musí umět integrovat a řídit nabíjecí stanice pro elektromobilitu, a to jak AC, tak DC stanice. Integrace zahrnuje i řízení v rámci komunitního sdílení a optimalizaci nabíjení v časech nákupů na DT a VDT.

1.12. Veřejné osvětlení

Aplikace umožňuje ovládat, nastavovat a řídit veřejné osvětlení, baterie spojené s tímto veřejným osvětlením, její nabíjení z přebytků FVE, sdílení nebo obchodování na DT a VDT. Jednotlivé HW prvky umožňují komunikovat minimálně protokolem DALI, optimálně i DALI2.

1.13. Integrovaná predikce výroby a spotřeby.

Dodaný systém musí mít integrovanou predikci výroby a spotřeby. Predikce musí poskytovat výpočty v podobě časových řad hodnot s obchodní periodou alespoň hodina s možností výhledu 15 minut. Výsledky predikce musí být uživatelsky přístupné v jednotném prostředí pro prohlížení a statistické zpracování všech dat z výroben, bateriových úložišť a spotřeb.

1.14. Vizualizace

Systém poskytuje rozhraní pro možnost vizualizace dodané dodavatelem nebo vlastní. Vizualizace umožňuje vytvořit např. dispečinkový systém, přehledné vizualizace pro jednotlivé vedoucí pracovníky, energetiky, ale i vizualizace pro prezentaci na webových stránkách, monitorech u vchodů a další. Vizualizace umožňuje i přepočty na tuny CO2 a počty ušetřených stromů. Vizualizace nesmí být omezená pouze na elektrickou energii, ale musí zobrazovat i ostatní energie, kotelny, rozvaděče, veřejné osvětlení. a další.
Přidanou hodnotou je editor vizualizací.

1.15. Alarmy, varování a notifikace

Systém umožňuje zasílání alarmů, varování a notifikací, jejich kvitování se záznamy časů vyvolání a kvitování. Možnosti odeslání jsou SMS, maily nebo notifikace v aplikaci. Všechny alarmy jsou volně definovatelné.

1.16. Napojení na podřízené lokální systémy

Systém musí mít možnost napojení na lokální řídící systémy pomocí datového rozhraní. Systém musí disponovat minimálně rozhraním DB-NET, MQTT, ModBus/TCP. Systém musí zohledňovat omezení jednotlivých lokalit, jako například velikost jističe, transformátoru, povolených výkonů a podobně.

1.17. Výkaznictví a automatizované reporty

Systém umožňuje automatizované vykazování statistik výroby licencovaných výroben na OTE přes rozhraní API. Systém taktéž umožňuje zasílat automatizované reporty v zadaných intervalech na definované mailové adresy.

1.18. Reporty provozu pro bilanční účely.

Poskytnutá aplikace musí umožnit uživatelsky sestavovat reporty provozu pro bilancování provozu technologie výroben, bateriových úložišť, spotřeb a všech dalších monitorovaných veličin. Bilanční periody jdou nastavit jakkoliv. Aplikace obsahuje uživatelské rozhraní pro definici grafů v jakémkoliv čase a s jakoukoliv ukládanou veličinou.

1.19. Export dat

Aplikace umožňuje jednoduchý export dat a grafů do standardních grafických a office formátů. Minimálně JPG, PNG, XLSX, XML a PDF.

1.20. Komunitní sdílení elektrické energie

Platforma musí podporovat možnost komunitního sdílení energie - správu členů, správu skupin sdílení, bilancování, rozdělení a návrhy priorit a % sdílení, fakturaci. Exporty a importy dat pro EDC, komunikaci pomocí API s EDC. Online orchestraci monitoringu a řízení zdrojů a spotřeb členů společenství pro co největší efektivitu výroby a spotřeby v rámci společenství. Systém podporuje všechny typy sdílení a jejich metody.

1.21. Lokální distribuční soustavy a mikrogridy

Platforma musí být schopna sběru dat a řízení vlastních LDS nebo mikrogridů pomocí protokolu „dlms“. Včetně napojení na monitoring LDS ČEZdistribuce. Systém umožňuje automatickou fakturaci, nebo odeslání podkladů pro fakturaci na zadané kontakty. Umožňuje jednotlivým uživatelům přístup k naměřeným datům v online režimu.

1.22. ESG (Environmental, Social and Corporate Governance) – udržitelnost, podpora a vykazování

Systém musí podporovat systém ESG, který v budoucnu budou města a obce vykazovat a dodržovat. A to jak v celku, tak na jednotlivých částech systému.

1.23. Spotové ceny, poskytování systémových služeb vyrovnávání rovnováhy

Systém umožňuje v rámci orchestrace systému, ale i v rámci řízení jedné lokality, řídit výrobu, spotřebu i dodávku na základě spotových cen, případně na základě pokynů ČEPS pro systémy SVR (služba vyrovnávání rovnováhy energie v síti). Využívá k tomu všechny dostupné zdroje, úložiště a spotřebiče, tak aby systém byl co nejefektivnější.

1.24. Automatizované analýzy

Systém umožňuje automatizovaně analyzovat a nacházet neefektivnosti pomocí datové analýzy. Případně je nápomocna při této činnosti energetikovi nebo jiným pověřeným uživatelům.

1.25. HW pro monitoring

Výhodou je, pokud poskytovatel nabídne typizovaný sériový HW pro monitoring a řízení jednotlivých lokalit.

1.26. Umělá inteligence

Systém bude připraven pro využití umělé inteligence. V řízení a orchestraci se to projeví ve výpočtových a prediktivních algoritmech tak, aby systém neustále prověřoval ekonomiku provozu celého systému, aby bral v potaz variabilitu a operabilitu aktuálního stavu. Umělá inteligence může časem přispět k novým modelům a provozním scénářům.

1.27. Systém scén a plánů

Aplikace v sobě obsahuje možnosti tvořit scénáře provozu, týdenní plány a případně další časové metody pro optimalizaci řízení a orchestraci celku.

2. Požadavky na servis a provoz

2.1. Monitoring provozu v Cloud službě po dobu minimálně 5 let.

Poskytnuté služby musí být pro uživatele dostupné po dobu minimálně 4 let ode dne uvedení do plného provozu. Poskytovatel musí garantovat dostupnost služeb nezávisle od technologie nebo poskytovatele cloudové technologie. Případné změny musí řešit poskytovatel samostatně bez dodatečného přenášení vyvolaných nákladů na přijímatele služby.

2.2. Archivace a uchování dat

Veškeré data musí být trvale a bez změn archivována minimálně po dobu **36** měsíců od času vzniku dat. Výhodou je bezeztrátová technologie a ukládání dat s neomezeným časovým rámcem.

2.3. Garantovaný servis

Poskytovatel musí pro uživatele nabídnout garantovaný servis formou převzetí a řešení vad v standardním pracovním čase od 07:00 do 15:30 v pracovní dny (doba přebírání incidentů na řešení). Jiné časy musí poskytovatel nabídnou jako rozšíření garance na vyžádání. Poskytovatel musí standardně nabídnout help-deskové webové prostředí pro zadávání tiketů a hot-line linku. Poskytovatel nabídne časy řešení pro dané incidenty a jejich ceny.

2.4. Garantovaný vývoj

Poskytovatel garantuje po dobu minimálně 5 let neustálý vývoj aplikace tak aby odpovídala platné legislativě a aby akceptovala vývoj nových funkcionalit a možností v energetice.

2.5. Uvedení do provozu

Předpokládá se zavedení systému od 1.4.2025. Veškeré požadované funkcionality musí být zprovozněny maximálně do 30.6.2025. Nedodržení těchto termínů bude považováno za zásadní porušení smluvních podmínek a smlouva může být ze strany zadavatele okamžitě vypovězena včetně uplatnění smluvní pokuty ve výši součtu nabídkových cen bez dph.

3. Bezpečnost

3.1. Ochrana dat

Všechna data týkající se energetického řízení musí být chráněna proti neoprávněnému přístupu, ztrátě nebo poškození. To zahrnuje šifrování dat při přenosu i v klidu.

3.2. Přístupová práva

Je nutné zavést přísné kontroly přístupu, aby pouze autorizovaní uživatelé měli přístup k systémům CŘE. To zahrnuje použití silných autentizačních metod, jako jsou dvoufaktorová autentizace a pravidelné aktualizace přístupových práv.

3.3. Monitorování a audit

Pravidelné monitorování a auditování systémů CŘE je klíčové pro detekci a reakci na bezpečnostní incidenty. To zahrnuje sledování logů, detekci anomálií a pravidelné bezpečnostní audity.

3.4. Kybernetická bezpečnost

Implementace firewallů, antivirových programů a dalších bezpečnostních opatření k ochraně systémů před kybernetickými útoky je nezbytná. Důležité je také pravidelné aktualizování softwaru a bezpečnostních záplat.

3.5. Školení zaměstnanců

Zaměstnanci by měli být pravidelně školeni v oblasti informační bezpečnosti, aby byli schopni rozpoznat a reagovat na potenciální hrozby. To zahrnuje školení o phishingu, bezpečném používání hesel a dalších bezpečnostních praktikách.

3.6. Soulad s legislativou

Všechny implementace musí být v souladu s platnými zákony a předpisy, jako je zákon o kybernetické bezpečnosti a GDPR, které stanovují požadavky na ochranu osobních údajů a bezpečnost informačních systémů.

3.7. Segmentace sítě

Oddělení sítí pro CŘE od ostatních IT systémů může minimalizovat riziko šíření kybernetických útoků. To zahrnuje použití virtuálních LAN (VLAN) a dalších technologií pro segmentaci sítě.

3.8. Zálohování dat

Pravidelné zálohování dat je klíčové pro obnovu systémů po případném útoku nebo selhání. Zálohy by měly být uloženy na bezpečném místě a pravidelně testovány.

3.9. Incident Response Plan (IRP)

Mít připravený a pravidelně aktualizovaný plán reakce na incidenty je nezbytné pro rychlou a efektivní reakci na bezpečnostní incidenty. Tento plán by měl zahrnovat kroky pro identifikaci, izolaci, řešení a obnovu po incidentu.

3.10. Bezpečnostní standardy a certifikace

Dodržování mezinárodních bezpečnostních standardů, jako jsou ISO/IEC 27001 pro řízení informační bezpečnosti, může pomoci zajistit, že jsou implementovány osvědčené postupy.

3.11. Pravidelné testování zranitelností

Provádění pravidelných penetračních testů a hodnocení zranitelností může pomoci identifikovat a opravit slabá místa v systémech CŘE.

3.12. Bezpečnostní politika

Vypracování a implementace komplexní bezpečnostní politiky, která definuje pravidla a postupy pro ochranu informačních systémů, je klíčová. Tato politika by měla být pravidelně revidována a aktualizována.

3.13. Bezpečnostní aktualizace

Pravidelné aktualizace softwaru a firmware jsou nezbytné pro ochranu systémů před nově objevenými zranitelnostmi. To zahrnuje nejen operační systémy, ale i veškeré aplikace a zařízení připojené k síti.

3.14. Fyzická bezpečnost

Zajištění fyzické bezpečnosti serverů a dalších klíčových zařízení je stejně důležité jako kybernetická bezpečnost. To zahrnuje kontrolu přístupu do serveroven, použití bezpečnostních kamer a dalších opatření.

3.15. Redundance a vysoká dostupnost

Implementace systémů s vysokou dostupností a redundancí může minimalizovat dopady případných výpadků. To zahrnuje použití záložních serverů, redundantních napájecích zdrojů a dalších opatření.

3.16. Bezpečnostní testování

Pravidelné provádění bezpečnostních testů, jako jsou penetrační testy a simulace útoků, může pomoci identifikovat a opravit slabá místa v systémech.

3.17. Incident Management

Mít jasně definovaný proces pro řízení bezpečnostních incidentů, včetně jejich hlášení, analýzy a nápravy, je klíčové pro minimalizaci dopadů bezpečnostních incidentů.

3.18. Bezpečnostní standardy

Dodržování mezinárodních bezpečnostních standardů, jako jsou NIST, ISO/IEC 27001 a další, může pomoci zajistit, že jsou implementovány osvědčené postupy a že systémy splňují požadované bezpečnostní normy.