

ReCON MES

Popis

ReCON MES je produkt, který slouží k vizualizaci dat získaných ze strojů. Pro správnou funkci tohoto produktu je nutné, aby byly stroje připojeny do podnikové sítě a byl aktivní přenos pomocí protokolů OPC UA nebo MTConnect. K uskutečnění tohoto sběru dat lze využít také produkt ReCON OPC UA.

ReCON MES pomocí vhodných algoritmů transformuje tato data do přehledných informací. Uživatel má možnost zobrazit si tyto informace buď online pro aktuální náhled, nebo je skládat do přehledných reportů. Tím umožňuje efektivní vizualizaci a analýzu dat ze strojů, což může pomoci vylepšit výkon a řízení výrobního procesu.

Možnosti nasazení

ReCON MES může být provozován jako cloudová služba na platformě Microsoft Azure, což zaručuje vždy nejnovější verze produktu. Alternativně je také možné provozovat ReCON MES jako on-premisovou aplikaci, která je nasazena v "lokálním cloudu". V případě on-premisového i cloudového řešení máte možnost využít fyzicky dodaný hardwarový systém od společnosti TAJMAC-ZPS, nebo můžete virtualizovat aplikaci na serveru u zákazníka.

Obě varianty umožňují provozovat ReCON MES v prostředí dle vašich potřeb a preferencí. Cloudová služba na Microsoft Azure zajišťuje aktualizace a správu produktu ze strany poskytovatele, zatímco on-premisové nasazení poskytuje větší míru kontroly nad infrastrukturou a umožňuje přizpůsobení produktu vašim interním požadavkům.

HW konfigurace pro virtuální server zákazníka

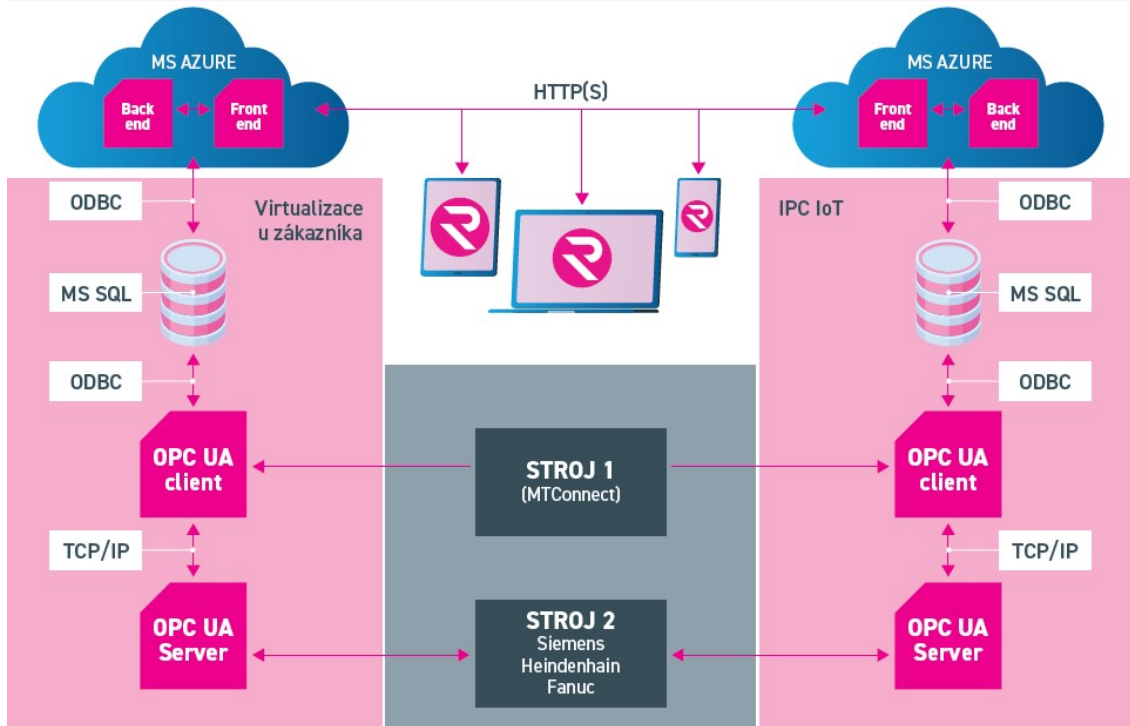
Je důležité prověřit HW konfiguraci pro virtuální server u zákazníka společně se správcem sítě. Tím zajistíte, že prostředky a požadavky na provoz ReCON MES budou splněny a systém bude správně fungovat.

Během tohoto procesu je vhodné diskutovat s poskytovatelem virtuálního serveru a správcem sítě o specifikacích a požadavcích Vašeho virtuálního sběrače ReCON OPC UA. Mezi faktory, které je třeba zvážit, patří výkon, dostupná paměť, síťová propustnost a další technické parametry, které ovlivňují provoz produktu.

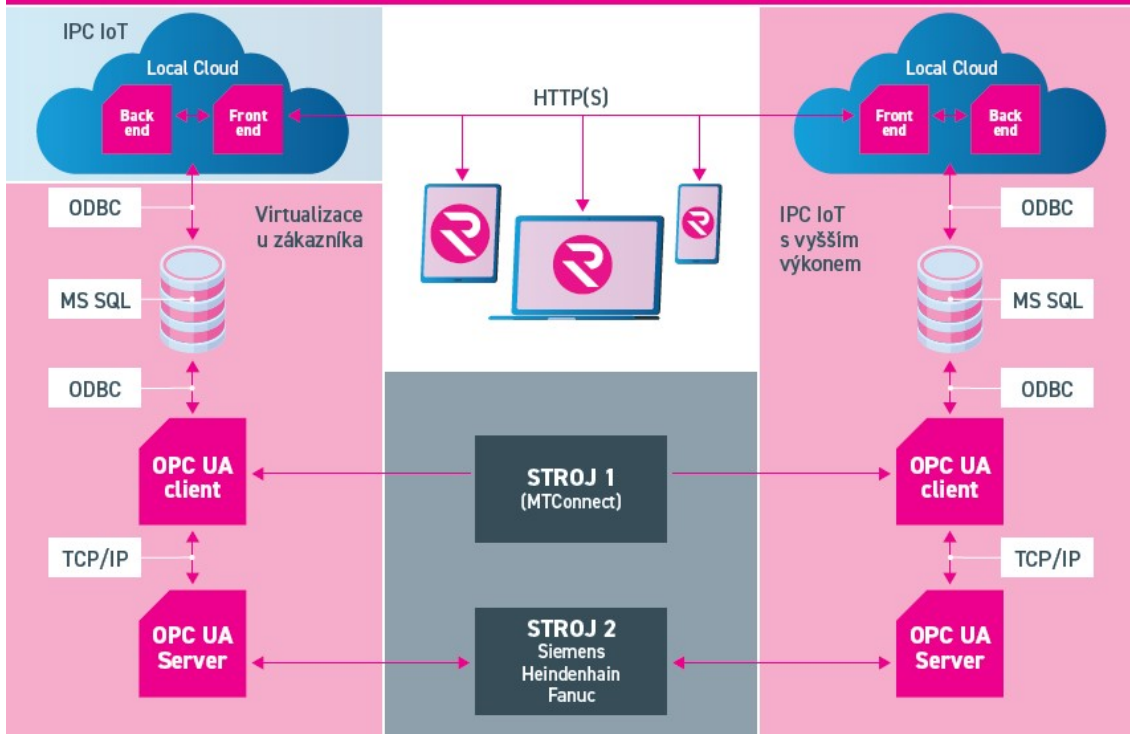
Spolupráce se správcem sítě a konzultace s poskytovatelem virtuálního serveru vám umožní zajistit, že virtuální sběrač ReCON OPC UA bude správně nakonfigurován a připraven pro sběr dat z Vašich strojů a tedy připraven pro ReCON MES a správnou vizualizaci těchto informací.

Technické řešení

ReCON MES - Cloudová varianta



ReCON MES - Onpremise varianta



Metody vyhodnocování

Vyhodnocování dat v rámci ReCON MES probíhá z dvojího zdroje sběru informací. Prvním způsobem je automatický sběr stavů strojů, který získává data o stavu strojů přímo ze sensorů nebo systémů monitorování. Tato metoda poskytuje kontinuální informace o aktuálním stavu strojů.

Druhým způsobem je manuální sběr stavu, který je prováděn obsluhou strojů. Tato metoda slouží k doplnění informací o důvodech prostojů, které automatický sběr sám o sobě nemusí zachytit. Obsluha strojů manuálně zadává informace o příčinách a důvodech prostojů, což umožňuje získat komplexnější pohled na celkový stav výrobního procesu.

Je důležité poznamenat, že manuální sběr stavu od obsluhy není nezbytně nutný pro fungování systému ReCON MES, ale slouží jako doplňkový zdroj informací pro detailnější analýzu a monitorování výrobních prostojů.

Připojení do podnikové sítě

V případě ReCON MES je nutné, aby výrobní zařízení poskytovala data ve formátu OPC UA datové věty, což vyžaduje přítomnost OPC UA serveru. Alternativně je možné využít také protokol MTConnect pro přenos dat.

To znamená, že ReCON MES bude schopen získávat a zpracovávat data z výrobních zařízení, která podporují tyto protokoly. V případě OPC UA bude komunikace probíhat přes OPC UA server, který je připojen ke všem příslušným strojům a umožňuje přenos dat. Proces sběru a zpracování dat v ReCON MES je závislý na těchto specifikacích a technologiích pro zajištění správné funkce a kompatibility s výrobním prostředím.

Nepřipojené pracoviště

Existují technologická pracoviště, která nemají přímé připojení prostřednictvím sítě, a proto je potřeba využít jiného způsobu sběru dat. V případě ReCON MES může být pro tyto pracoviště vytvořen NFC tag, který slouží k manuálnímu sběru dat.

Obsluha pracoviště se pomocí NFC tagu přihlásí na konkrétní výrobní operaci. Tímto způsobem může ReCON MES sledovat, jak dlouho daná operace trvá a kolik kusů bylo na ní vykázáno. Tyto informace jsou pak zaznamenány a použity pro analýzu a monitorování výrobního procesu.

Tato metoda sběru dat prostřednictvím NFC tagů umožňuje sledovat výkonnost a produktivitu technologických pracovišť, i když nejsou připojena přímo k podnikové síti. ReCON MES dokáže integrovat a zpracovávat tyto manuálně sbírané informace společně s ostatními daty, poskytující tak komplexní pohled na výrobní proces.

Monitoring montáže

Podobným způsobem je možné monitorovat i montážní operace, pokud jsou k dispozici. Pro tyto operace lze vytvořit NFC tagy nebo jiná identifikační zařízení, která umožňují obsluze přihlásit se ke konkrétní montážní operaci.

S pomocí těchto identifikačních zařízení lze sledovat, jak dlouho trvá jednotlivé montážní operace a kolik kusů bylo vyrobeno. Tato data pak mohou být sbírána a integrována do ReCON MES, kde jsou zpracovávána a analyzována. Tímto způsobem je možné sledovat a vyhodnocovat výkonnost montážních operací, identifikovat případné problémy nebo zlepšovat efektivitu výrobního procesu.

Díky ReCON MES lze tedy nejen sledovat stroje, ale také monitorovat montážní operace a získávat cenné informace pro optimalizaci výrobního prostředí.

Kyberbezpečnost

V souvislosti s kyberbezpečností je důležité si uvědomit, že jakékoli zařízení nebo systém, který je zapojen v podnikové síti zákazníka, včetně ReCON MES, podléhá platným normám a požadavkům v oblasti kyberbezpečnosti.

Zákazník je odpovědný za zajištění bezpečnosti své podnikové sítě a systémů a měl by přijmout opatření a postupy k minimalizaci rizika kybernetických hrozeb a zranitelností. To zahrnuje správné nastavení sítě, použití silných autentizačních mechanismů, aktualizace a správu softwarových a hardwarových komponent, monitorování a detekci neoprávněného přístupu a dalších bezpečnostních opatření.

Dodavatel systému ReCON MES může poskytnout informace o bezpečnostních funkcích a doporučeních pro jeho správnou instalaci a provoz, ale konečná odpovědnost za kyberbezpečnost v rámci podnikové sítě leží na zákazníkovi samotném.

Zákazník by měl přijmout vlastní kyberbezpečnostní politiku, která zohledňuje specifika jeho podnikové sítě a požadavky na ochranu dat a systémů. Měl by také pravidelně monitorovat a aktualizovat bezpečnostní opatření a sledovat nové trendy a hrozby v oblasti kyberbezpečnosti.

Dodavatel ReCON MES by měl spolupracovat se zákazníkem a poskytnout příslušné informace, dokumentaci a technickou podporu, která pomůže zákazníkovi splnit jeho požadavky na kyberbezpečnost v rámci nasazení.

V zájmu zachování bezpečnosti je důležité, aby zákazník i dodavatel dodržovali platné normy a postupy kyberbezpečnosti a spolupracovali při identifikaci, prevenci a řešení bezpečnostních rizik spojených s nasazením ReCON MES v podnikové síti.

Samotná komunikace mezi výrobním zařízením/strojem a sběračem probíhá pomocí TCP/IP protokolu. Komunikace na MS AZURE nebo Local cloudem dále probíhá pomocí šifrovaného protokolu ODBC (standart Microsoft). Zabezpečení informací na MS AZURE vyplývá z licenčních podmínek při použití této služby.

Webová aplikace jako taková a její zobrazení informací je provedeno pomocí HTTPS šifrovaného protokolu, popřípadě VPN zákazníka.

Veškerá data jsou uložena buďto na fyzické HW od TAJMAC-ZPS pomoci MS SQL databáze, nebo jsou na virtuálním serveru opět pomocí MS SQL databáze.

Předání do užívání

Konfigurace a instalace: Po dodání ReCON MES systému od společnosti TAJMAC-ZPS je nutné provést jeho konfiguraci a instalaci. To zahrnuje připojení ke sběrači OPC UA či MTConnect.

Součástí předávacích dokumentů je:

Prohlášení o autorství ReCON MES

Smlouva k užívání ReCON MES

Předávací protokol ReCON MES

Rámcová nabídka ReCON MES

Integrace dat z programů třetích stran

Integrace dat z programů třetích stran může být složitý proces, protože vyžaduje propojení a synchronizaci dat mezi různými systémy a subjekty. Je třeba zohlednit různé proměnné veličiny a přizpůsobit integraci konkrétním potřebám a požadavkům.

Je vhodné komunikovat s dodavatelem systému ReCON MES a případně s dodavatelem programů třetích stran, abyste zajistili úspěšnou integraci dat a dosáhli požadovaných výsledků. Tuto komunikaci z pravidla zajišťuje koncový zákazník.

Vzdálená technická podpora

Pro poskytování vzdálené technické podpory je nutné zajistit spojení s HW nebo virtuálním serverem. Zde jsou minimální technické požadavky na připojení k internetu pro výkon vzdálené plochy:

Minimální rychlost připojení: Doporučuje se šířka pásma s minimální rychlostí 10 Mbps pro stabilní a plynulý provoz vzdálené plochy. Nicméně, optimální rychlost závisí na konkrétních potřebách a nárocích na přenos dat.

Nízká odezva (latence): Nízká latence je důležitá pro rychlou a plynulou odezvu při vzdálené práci. Doporučuje se minimální latence pod 100 ms, ale opět záleží na konkrétních požadavcích.

Stabilita připojení: Připojení by mělo být stabilní a bez častých výpadků. Výpadky a nestabilita mohou negativně ovlivnit kvalitu vzdálené plochy a technickou podporu.

Bezpečnostní opatření: Pro zabezpečení připojení by se měly používat vhodné bezpečnostní protokoly, jako je VPN (Virtual Private Network), který zajišťuje šifrovanou komunikaci mezi vzdáleným zařízením a HW.

Otevření portů: V případě, že se zákazník rozhodne připojit se přes veřejné internetové spojení, je třeba otevřít specifický port pro komunikaci s HW ve firewallu nebo v routeru. Je nutné zajistit, aby byl tento port správně nakonfigurován a zabezpečen.

Přiměřená šířka pásma pro provoz: Závisí na množství prováděných operací a přenosu dat během vzdálené podpory. Vyšší šířka pásma může zlepšit rychlost a plynulost přenosu dat.

Je důležité konzultovat tyto technické požadavky s dodavatelem ReCON MES a provést analýzu nároků na připojení k internetu pro vzdálenou plochu, aby byla zajištěna optimální a bezproblémová vzdálená technická podpora.

Pokud je vyžadována fyzická přítomnost technické podpory u zákazníka a nelze využít vzdáleného přístupu, takové služby jsou obvykle zpoplatněny podle aktuálního ceníku společnosti TAJMAC-ZPS, pokud není ve smlouvě stanoveno jinak.

Záruční podmínky

Odpovědnost dodavatele není zahrnuta v situacích, kdy výrobní zařízení přestane posílat data z důvodu nefunkčnosti jeho systému, špatného nastavení, umyšleného přepisu komunikačního rozhraní ve výrobním zařízení nebo závady v komunikaci podnikové sítě.

Dodavatel nenese odpovědnost za chyby, které jsou způsobeny faktory mimo jeho kontrolu a odpovědnostní oblast. To zahrnuje problémy, které mohou vzniknout na straně výrobního zařízení, jeho systému, nastavení nebo komunikační infrastruktury, která není součástí dodávky systému ReCON MES.

V těchto případech je odpovědnost za řešení a odstranění problémů na straně výrobního zařízení, jeho systému, nastavení nebo komunikační infrastruktury na zákazníkově nebo jiných odpovědných stranách.

Je důležité, aby zákazník měl v souladu se svými potřebami a požadavky správně nakonfigurováno výrobní zařízení, jeho systém, nastavení a komunikační infrastrukturu, aby zajistil správnou a bezproblémovou komunikaci mezi výrobním zařízením a sběračem ReCON OPC UA.

Tímto je upozorněno, že dodavatel neodpovídá za nefunkčnost, která je mimo jeho kontrolu a odpovědnostní oblast, a zákazník je zodpovědný za správné nastavení a provoz výrobního zařízení a souvisejících systémů.

Záruční podmínky pro HW

Záruka na veškerý dodaný hardware od společnosti TAJMAC-ZPS je standardně poskytována po dobu 1 roku, pokud v kupní smlouvě není uvedeno jinak. Tato záruka zajišťuje, že dodaný hardware je v souladu se specifikacemi a bude fungovat správně po dobu jednoho roku od data nákupu.

Je důležité si uvědomit, že záruka na hardware se vztahuje pouze na fyzické vady nebo chyby, které jsou způsobeny výrobou nebo manipulací při dopravě. Záruka se nevztahuje na škody způsobené nesprávným použitím, úmyslným poškozením, přetížením, nevhodným napájením nebo připojením nebo jiným nedodržením návodů nebo pokynů pro použití.

V případě potřeby uplatnění záruky na dodaný hardware je nutné postupovat podle stanovených podmínek, které jsou obvykle uvedeny v záručním listu nebo dokumentaci k produktu. V těchto případech je vhodné kontaktovat přímo společnost TAJMAC-ZPS, aby bylo zahájeno řešení reklamace či opravy.

Je vždy doporučeno důkladně prozkoumat a porozumět záručním podmínkám a ustanovením v konkrétní kupní smlouvě, protože ty mohou specifikovat odlišnou dobu záruky nebo další podmínky, které by měly být dodrženy.

Záruční podmínky pro virtuální server

Při použití sběrače na virtuálním serveru zákazníka je důležité pravidelně provádět zálohy. To platí i v případě, že sběrač využívá možnosti MS SQL databáze.

Zálohování je klíčové pro zajištění integrity a dostupnosti dat. Pravidelné zálohy serveru a databáze pomáhají minimalizovat riziko ztráty dat v případě hardwarového selhání, chyby v systému, nebo jiných nečekaných událostí.

Při využití MS SQL databáze je možné využít nástroje a funkce, které tato databáze nabízí pro zálohování a obnovu dat. Můžete například nastavit automatické plánování zálohování, definovat frekvenci a umístění záloh, a provádět obnovu dat z těchto záloh v případě potřeby.

Pokud je systém provozován na serveru zákazníka a ten jeho zásahem jakkoliv naruší integritu tohoto serveru, je povinen dodavatele o tomto informovat a konzultovat další postup a následné obnovení.

Tato činnost je brána nad rámec záruky a je fakturována.

