

Sedm základních prvků pro energetiku a veřejné služby

Organizace v oblasti energetiky a veřejných služeb očekávají, že budou mít prospěch z provozních zlepšení, protože urychlí svou digitální transformaci a zavedou inovace. Stále však budou čelit problémům, jako jsou strategie migrace, zastaralé technologie, integrace mezi novými a starými systémy a správa velmi rozsáhlých sítí.

Tento problém však může pomoci překonat sbližování provozních technologií (OT) a informačních technologií (IT), masivní nasazení internetu věcí (IoT) a průmyslového internetu věcí (IIoT) spolu s automatizací procesů a preventivní údržbou. Zde je sedm základních prvků, které je třeba zvážit.

1 Chraňte své lidi a majetek.

- Propojte zařízení, snímače, kamery, IoT a IIoT s [centrem řízení provozu](#).
- Zlepšete spolupráci mezi techniky na pracovišti a vzdálenými odborníky tím, že umožníte hlasové a video relace a sdílení dokumentů.
- Rychle identifikujte naléhavé situace, varujte před nimi, reagujte na ně a koordinujte je prostřednictvím centra řízení provozu.



2 Pracujte bez problémů v extrémních podmínkách.

- Zajistěte kontinuitu služeb ve všech prostředích díky implementaci robustních, redundantních [kritických sítí](#) a komunikačních systémů.
- Používejte [průmyslové přepínače](#) certifikované tak, aby odolaly extrémním teplotám, elektromagnetickému rušení, vlhkosti, vibracím, prachu a dalším vlivům, což snižuje požadavky na údržbu.
- Bezpečně připojte a spravujte širokou škálu zařízení IIoT, a to i v drsných a náročných prostředích.



3 Ovládejte svá připojená zařízení.

- Zajistěte bezpečné zaškolení zařízení [IoT](#) a IIoT a zároveň zabezpečte síť prostřednictvím segmentace IoT.
- Automatizujte nasazení sítě, zjednodušte úkoly, jako je přesouvání, přidávání a změny, a poskytněte pokročilé protokoly a funkce, jako je Shortest Path Bridging (SPB) pro mikrosegmentaci.
- Vytvořte vícekanálový pracovní postup pro oznamování mezi lidmi, procesy a snímači.



4 Chraňte před kybernetickými útoky a narušením.

- Zmírněte kybernetické hrozby implementací strategie [zabezpečení sítě s nulovou důvěrou](#).
- Zajistěte integrovanou kybernetickou bezpečnost pro kancelářské i vzdálené uživatelské aplikace.
- Vylepšete zabezpečení komunikačního systému pomocí šifrování hlasu a integrovaných bezpečnostních funkcí.



5 Dosáhněte sbližování OT-IT.

- Efektivně shromažďujte a distribuujte datové toky pro zpracování v reálném čase.
- Povolte vzdálené monitorování a řízení elektrických obvodů, ventilů a dalších [zařízení OT](#).
- Usonadněte mobilitu zaměstnanců na pracovišti zajištěním řešení DECT a Voice over Wi-Fi v souladu s oborovými předpisy.



6 Optimalizujte svůj provoz pro časovou a nákladovou efektivitu.

- Implementujte [jednotný systém správy sítě](#) pro kabelovou a bezdrátovou infrastrukturu a chraňte provoz v rámci dohledu a získávání dat (SCADA).
- Proaktivně řešte problémy se sítí pomocí [prediktivní údržby](#) a umělé inteligence a zajistěte včasnou detekci a řešení problémů.
- Zvažte modely OpEx a CapEx pro efektivní řízení omezení rozpočtu.



7 Minimalizujte spotřebu energie a dopad na životní prostředí.

- Zaveďte architektury a životní cykly produktů optimalizované pro maximální životnost.
- Využijte cloudová řešení, která snižují požadavky na prostor a energii.
- Zmírněte digitální znečištění, zlepšete nakládání s odpady a snižte [spotřebu energie](#) v celém hodnotovém řetězci.

Zjistěte více o tom, jak vám společnost Alcatel-Lucent Enterprise může pomoci:

Zlepšení bezpečnosti
a zabezpečení

Zvýšení efektivity
provozu

Zlepšení zapojení
zákazníků

Navštivte naše [webové stránky věnované energetice a veřejným službám](#).