

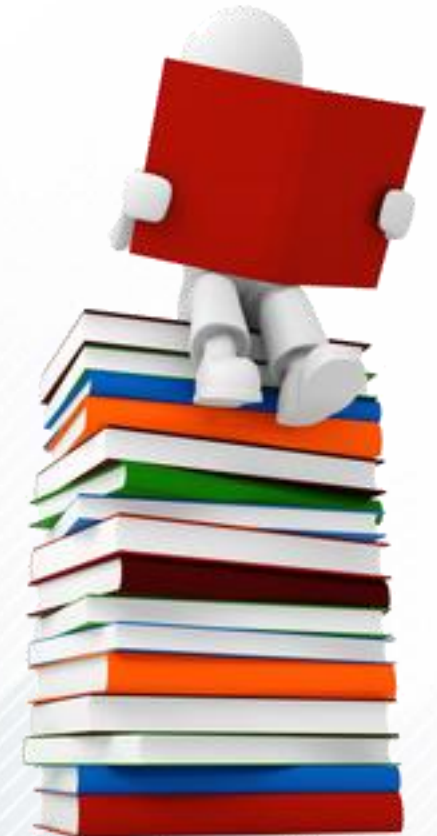
AVEVA a zásady kybernetické bezpečnosti

Pilíře kybernetické bezpečnosti realizované v SW AVEVA

Pavel Průša, Pantek (CS) s.r.o.

Obsah prezentace

- ▶ Kybernetická bezpečnost a ICS (průmyslové řídicí systémy)
- ▶ Zásady kybernetické bezpečnosti realizované v SW AVEVA
- ▶ Autentizace, autorizace
- ▶ Šifrovaná komunikace, certifikáty
- ▶ Podpora bezpečného uspořádání sítě
- ▶ Ubránitelný systém
- ▶ Otázky ... a odpovědi

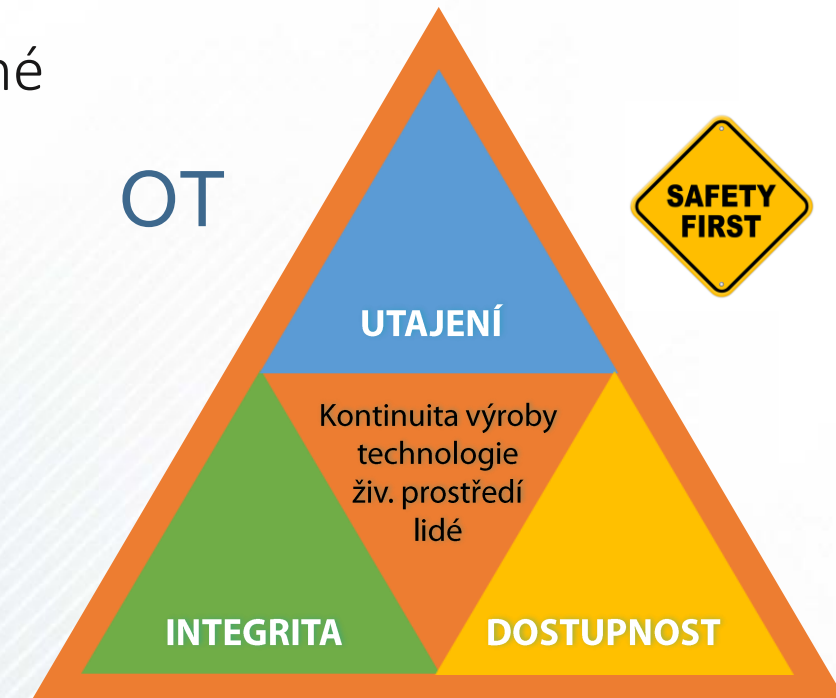
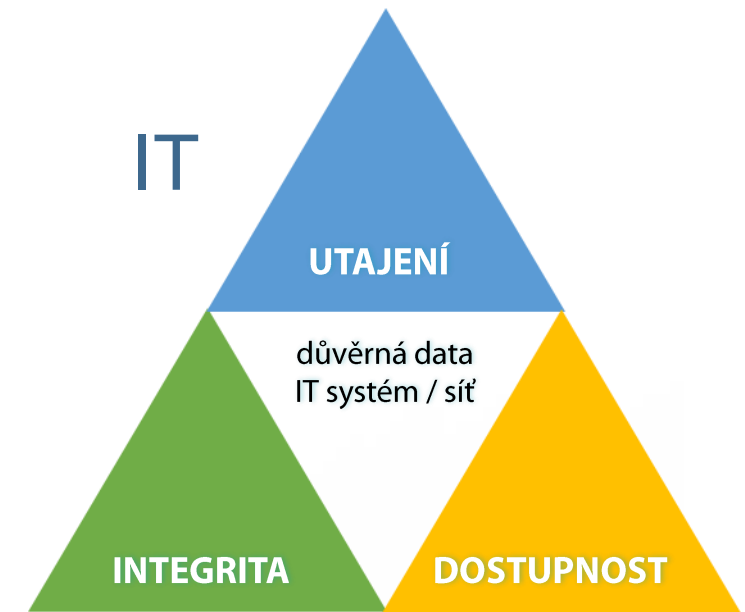


| Kybernetická bezpečnost a ICS

ICS = průmyslové řídicí systémy

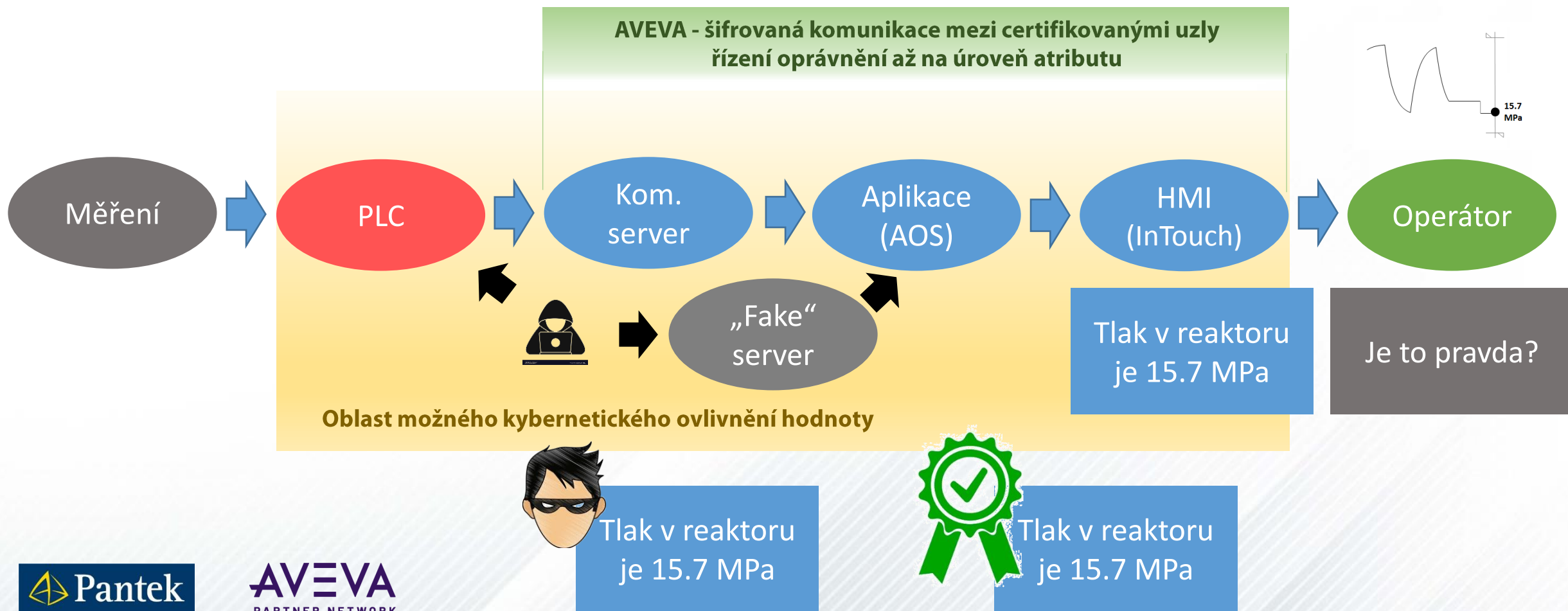
Kybernetická bezpečnost a ICS

- ▶ Klasický IT model nevystihuje zcela potřeby ICS
- ▶ Průmyslové systémy mají přesah do fyzického světa
 - ▶ Priorita – BEZPEČNOST, výrobní kontinuita
- ▶ Útoky na průmyslové systémy
 - ▶ Stuxnet, ukrajinský blackout.... meziročně 40% nárůst
 - ▶ Často velmi dobře promyšlené, naplánované, financované
- ▶ Změna paradigmatu v ochraně ICS
 - ▶ Nejde již jen o ochranu dat a sítě (IT pojetí)
 - ▶ Předmětem ochrany je samotný řídící systém, technologie, řízené procesy, prostředí, lidé



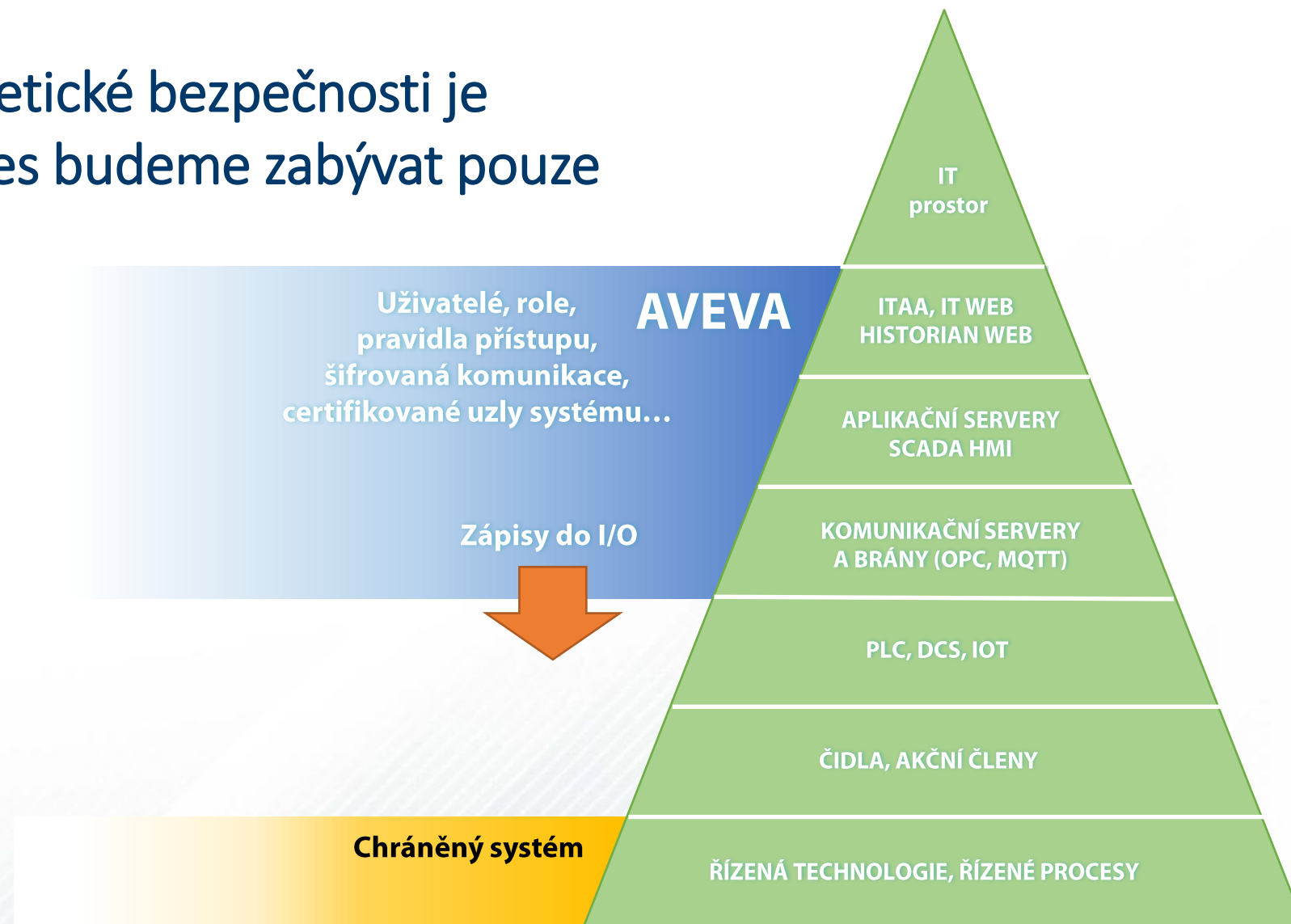
Důvěryhodnost = integrita + autenticita

- ▶ Nelze-li doložit integritu a autenticitu hodnoty, je tato hodnota NEJISTÁ
- ▶ Kdo / co nám tu hodnotu vlastně sděluje?



Pozice SW AVEVA v ICS

- Problematika kybernetické bezpečnosti je komplexní, my se dnes budeme zabývat pouze přínosy AVEVA SW



| Zásady kybernetické bezpečnosti realizované v AVEVA SW

Zásady kybernetické bezpečnosti realizované v AVEVA SW

- ▶ **Autentizace, Autorizace, Approval (= schválení), Audit (4xA)**
 - ▶ Systém – zpracování – vizualizace – oblast – objekt – atribut
 - ▶ Propojení s ActiveDirectory
- ▶ **Provoz klientských aplikací s oprávněním obyčejného uživatele**
- ▶ **Šifrovaná komunikace a identifikace uzlů systému**
 - ▶ System Management Server, certifikáty
- ▶ **Podpora vhodné síťové infrastruktury**
 - ▶ Secure Gateway, reverzní proxy, protokolové brány
 - ▶ Pouze odchozí propojení z DMZ

| Autentizace, autorizace...

Řízení oprávnění až na úroveň atributu

Autentizace, autorizace, schválení, audit v AVEVA System Platform

SYSTÉM ŘÍZENÍ OPRAVNĚNÍ V AVEVA SYSTEM PLATFORM

Autentizační mód

- Default / Galaxy / OS User / OS Group

Uživatelské role

- Role v Galaxy / OS nebo AD skupiny
- Práva pro vývoj a provoz

Oblasti zabezpečení

- Skupiny objektů

Objekty

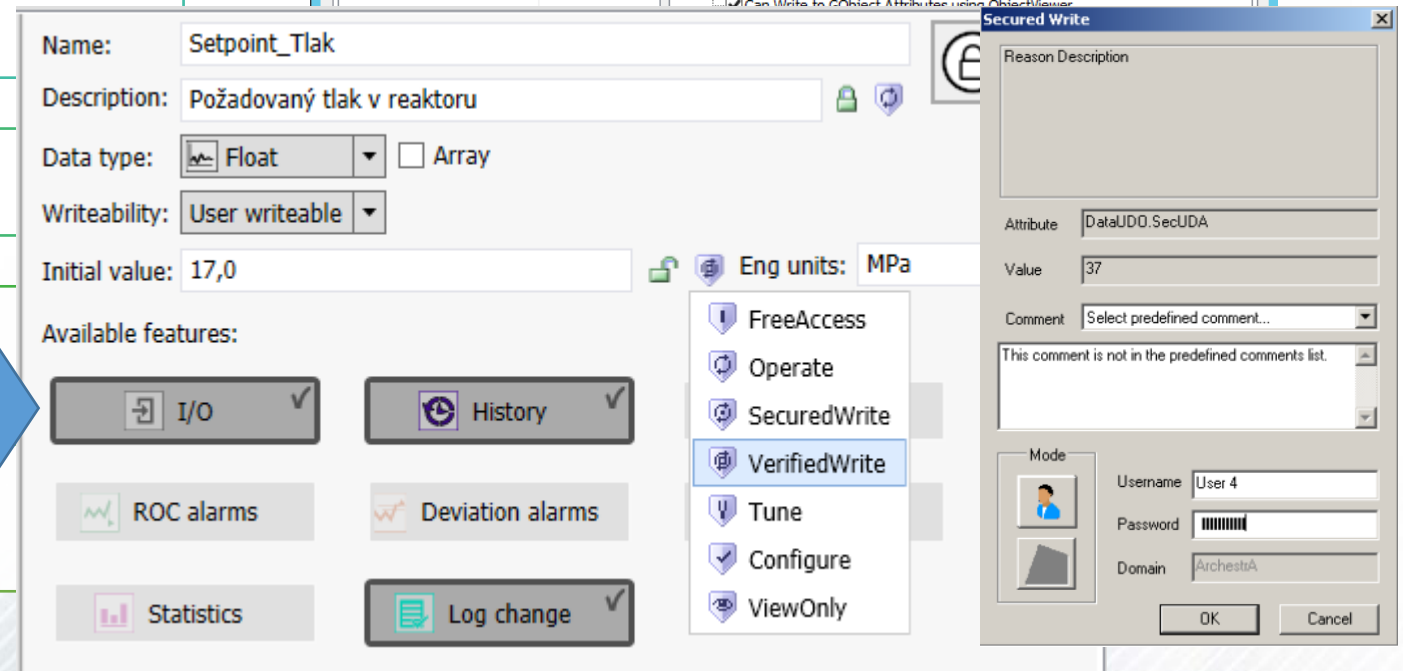
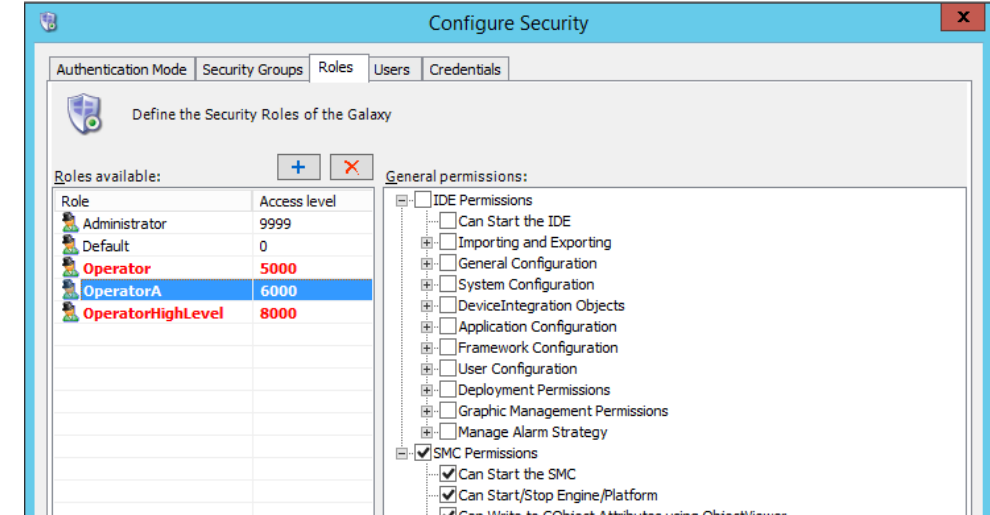
- Šablony a instance

Typy atributů z hlediska zápisu

- User Writeable / Object Writeable / Calculated / Locked

Politiky pro uživatelsky zapisovatelné atributy

- Free Access / Operate / Tune / Configure / Read Only
- Secured Write / Verified Write

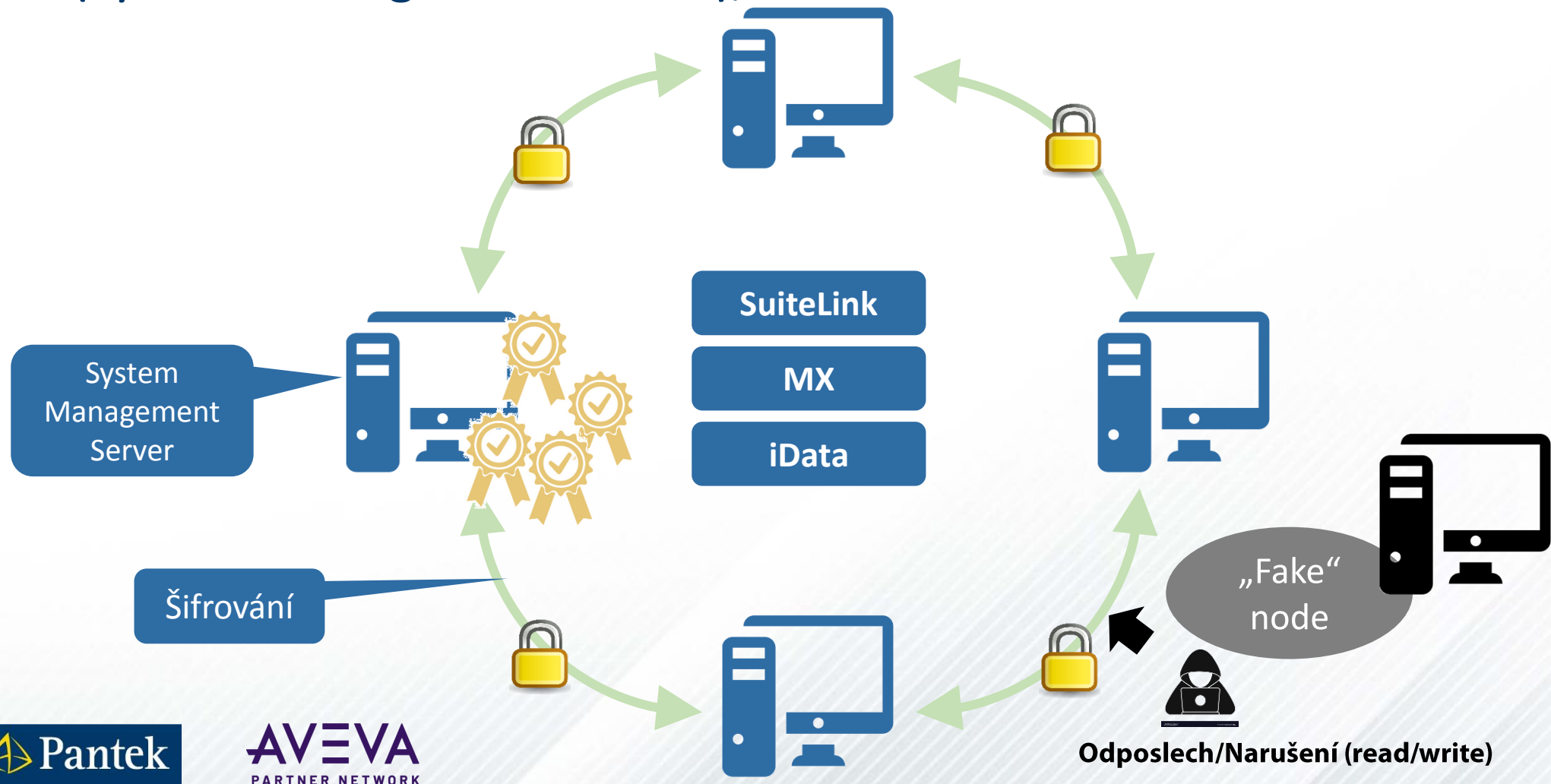


| Šifrovaná komunikace, certifikáty

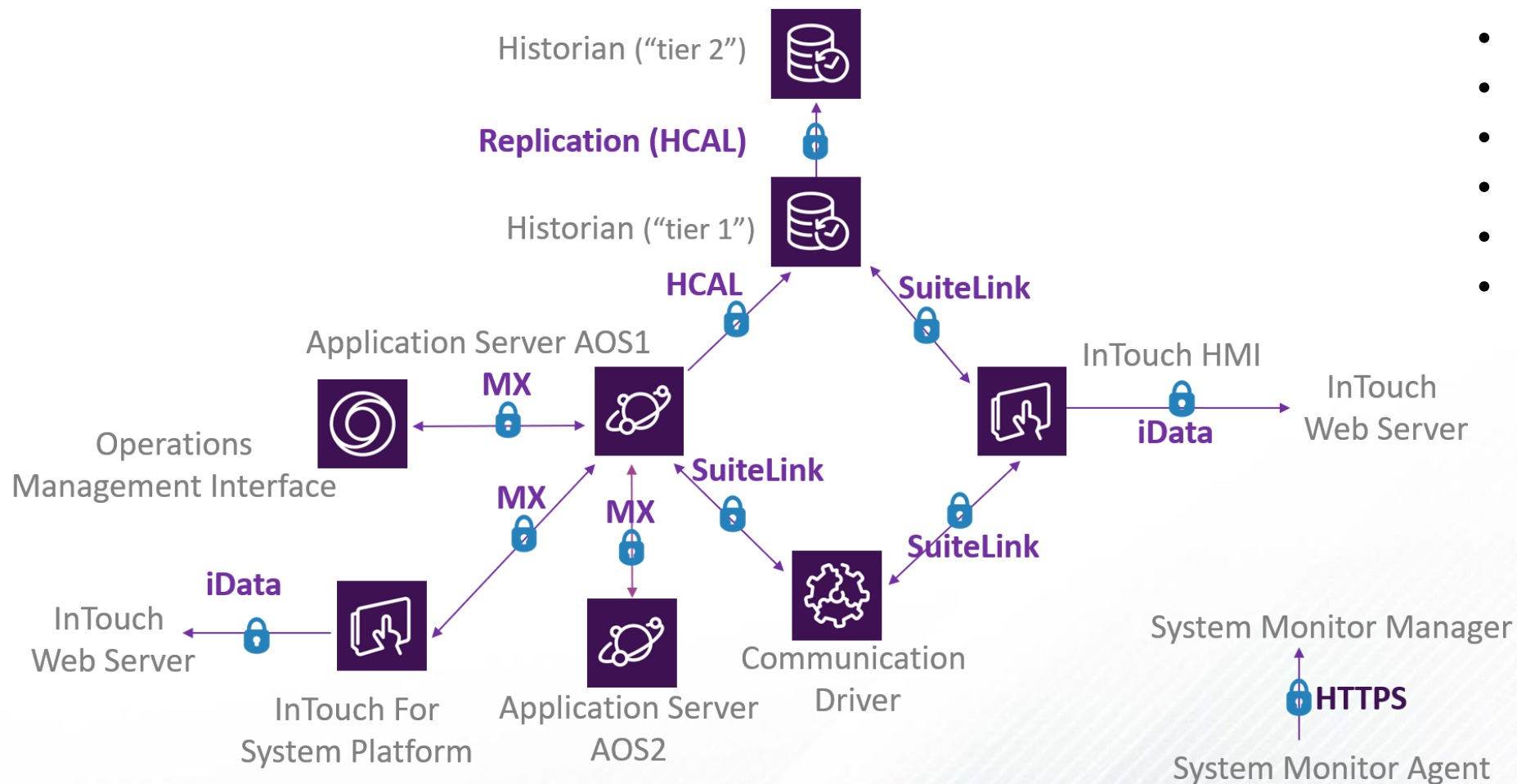
System Management Server
Certifikace uzlů systému

Šifrovaná komunikace, certifikáty

- ▶ Uzel, který se nemůže prokázat svou identitu certifikátem vydaným SMS (System Management Server), nemůže komunikovat s ostatními



Šifrovaná komunikace – dotčené protokoly



- SuiteLink
- Message Exchange (MX)
- iData
- iBrowser
- HCAL
- HTTPS

System Management Server

1 zvolený uzel

ostatní nasměrovány na zvolený SMS

Configurator

File Help

- AVEVA Enterprise Licensing Platform
- AVEVA Enterprise License Se
- AVEVA Historian
 - Server
- Reporting
- AVEVA System Monitor
 - System Monitor Manager
 - Alert Email Server
- AVEVA System Platform
 - Galaxy License Mode
- Common Platform
 - System Management Server**
- Industrial Graphics Server
 - Client Settings
 - Authentication Settings

Machines running AVEVA software must be configured to trust each other so that encrypted communications can be utilized. This is done by connecting them to a System Management Server.

☐ Connect to an existing System Management Server.

☒ This machine is the System Management Server.
There should only be one System Management Server in your topology for all AVEVA products. All other machines should be configured to connect to this System Management Server.

When configuring other machines, you should validate that the security code shown in the Configurator matches:

F2 BA 93 B5 0F 59 4A F2 BF 47 10 A8 77 01 E8 56 C9 E1 2B 2D

☐ No System Management Server configured. (NOT RECOMMENDED)
This option also allows you to remove any existing certificates that were managed by the System Management Server.

You can connect to a System Management Server by selecting the appropriate option in the left pane and then clicking the Advanced button.

Configuration Message: Flex License mode status: Flex License mode status:

Advanced Configuration

Certificates

In order to enable communications via encrypted channels (e.g. HTTPS), certificates must be configured.

Certificates can either be provided by your IT department or automatically generated.

Please select the appropriate options below.

Certificate Source: Automatically Generated

Certificate: WIN-VD56FUB3SF5 ASB

Ports

The common platform, and certain other AVEVA software (using "web port sharing" technology), communicate over web ports.

Please select the appropriate port to use on this machine.

HTTP Port: 80

HTTPS Port: 443

Certificate

General Details Certification Path

Certification path

- WIN-VD56FUB3SF5 ASB Root CA
- WIN-VD56FUB3SF5 ASB CA
- WIN-VD56FUB3SF5 ASB

View Certificate

Certificate status:

This certificate is OK.

OK

Refresh All Messages

System Management Server

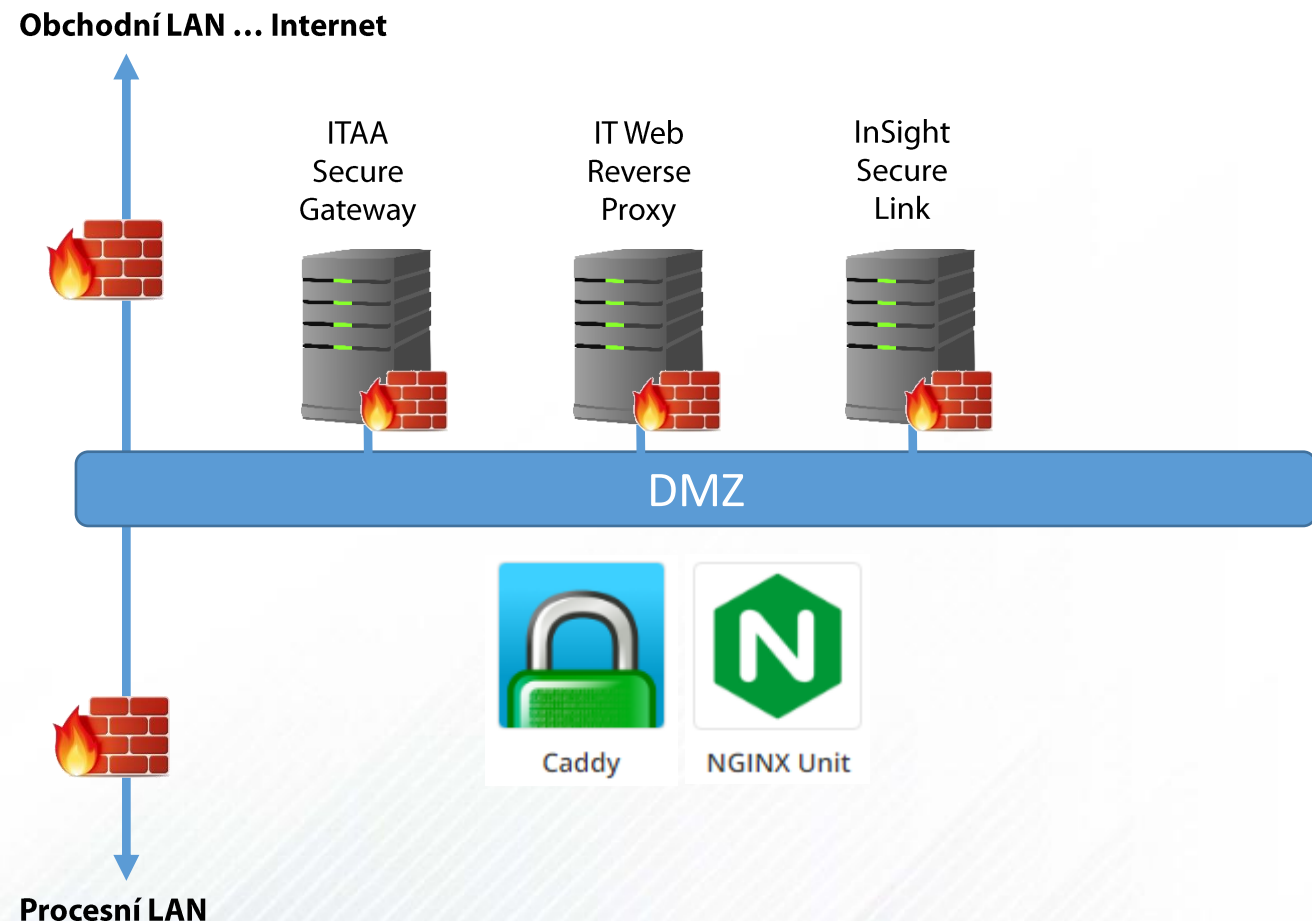
- ▶ Privátní certifikační autorita (CA) pro uzly AVEVA
- ▶ Šifrovaná komunikace TLS 1.2 mezi uzly, které „se vzájemně znají“
- ▶ **Certifikát = průkaz identity**
 - ▶ Certifikáty (root + ID uzlů systému) jsou generovány automaticky (SMS) nebo je root certifikát vydán certifikační autoritou (Verisign apod.)
 - ▶ Certifikát poskytnutý CA
 - ▶ Expiruje, ale snadno pokryje i uzly bez AVEVA SW – např. klienty IT Web Serveru
 - ▶ Automaticky generovaný
 - ▶ Automatická obnova, na uzlech bez AVEVA SW je třeba jej zdůvěryhodnit
- ▶ **Certifikované uzly**
 - ▶ Spolu mohou komunikovat pouze uzly nasměřované na stejnou CA / SMS
 - ▶ Vyloučení útoků typu „Man In The Middle“

| Podpora bezpečného uspořádání sítě

Brány pro nasazení v DMZ

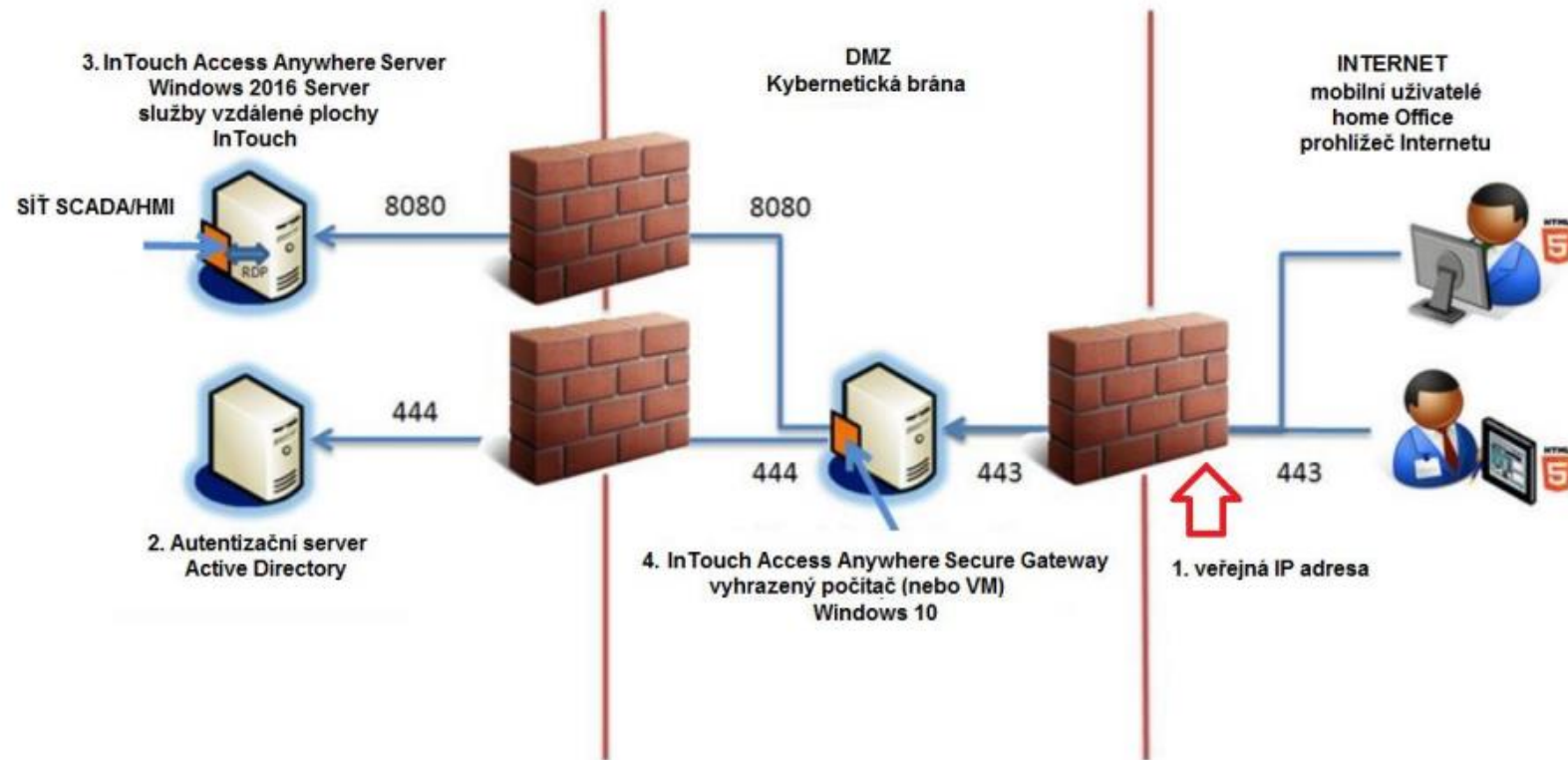
Podpora vhodného uspořádání sítě

- ▶ Segmentace sítě včetně DMZ
- ▶ DMZ brány
 - ▶ ITAA Secure Gateway
 - ▶ TLS – HTTPS
 - ▶ InTouch Web Reverse Proxy
 - ▶ NGINX
 - ▶ CADDY
 - ▶ InSight Secure Link
- ▶ Pouze odchozí spojení „ven“



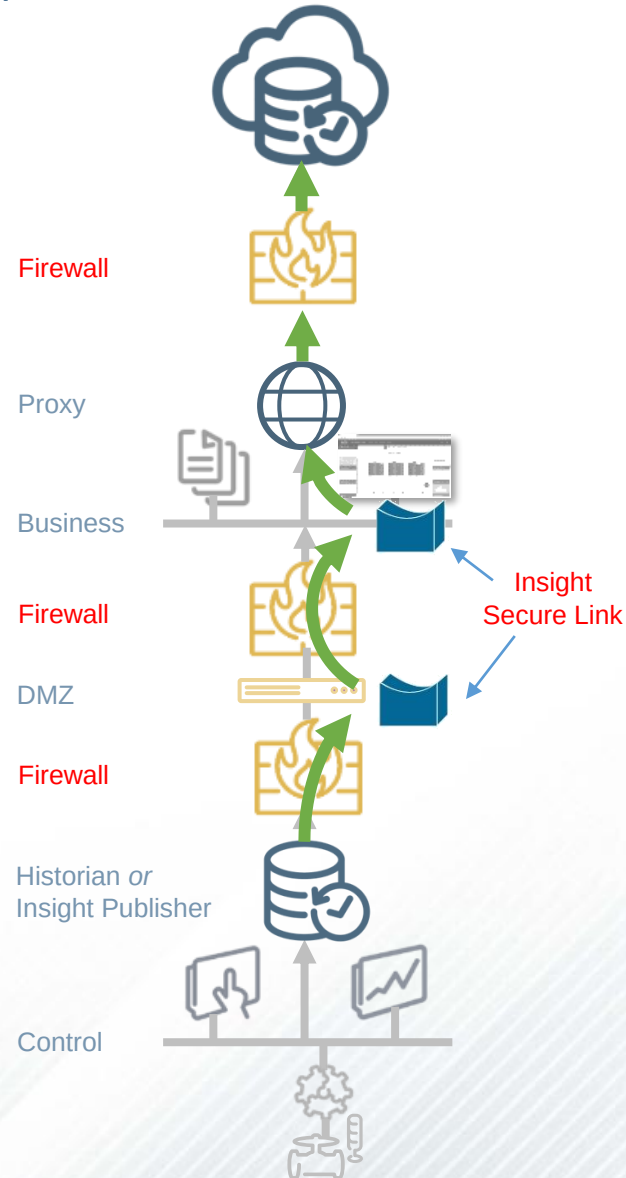
ITAA Secure Gateway

- ▶ Obrázek z dokumentu Pantek (CS)
 - ▶ ITAA – jak snadno začít



Insight Secure Link (ISL)

- ▶ Jednosměrný „bridge“
 - ▶ Jediný odchozí port
 - ▶ Žádná příchozí spojení
- ▶ Provoz šifrován TLS
- ▶ DMZ
- ▶ ISL je možné řetězit



Insight Secure Link AVEVA

Incoming Connections

The bridge will wait for connections from your Insight Publishers

Address Port

Make note of the IP address and port selected above-you will need to enter them for the Insight Publisher's "Web Proxy Configuration."

[← Back](#) [Continue](#)

Insight Secure Link AVEVA

Outgoing Connections

☒ Forward to upstream proxy
Indicates that there is another proxy that needs to be straddled in order to connect to the internet.

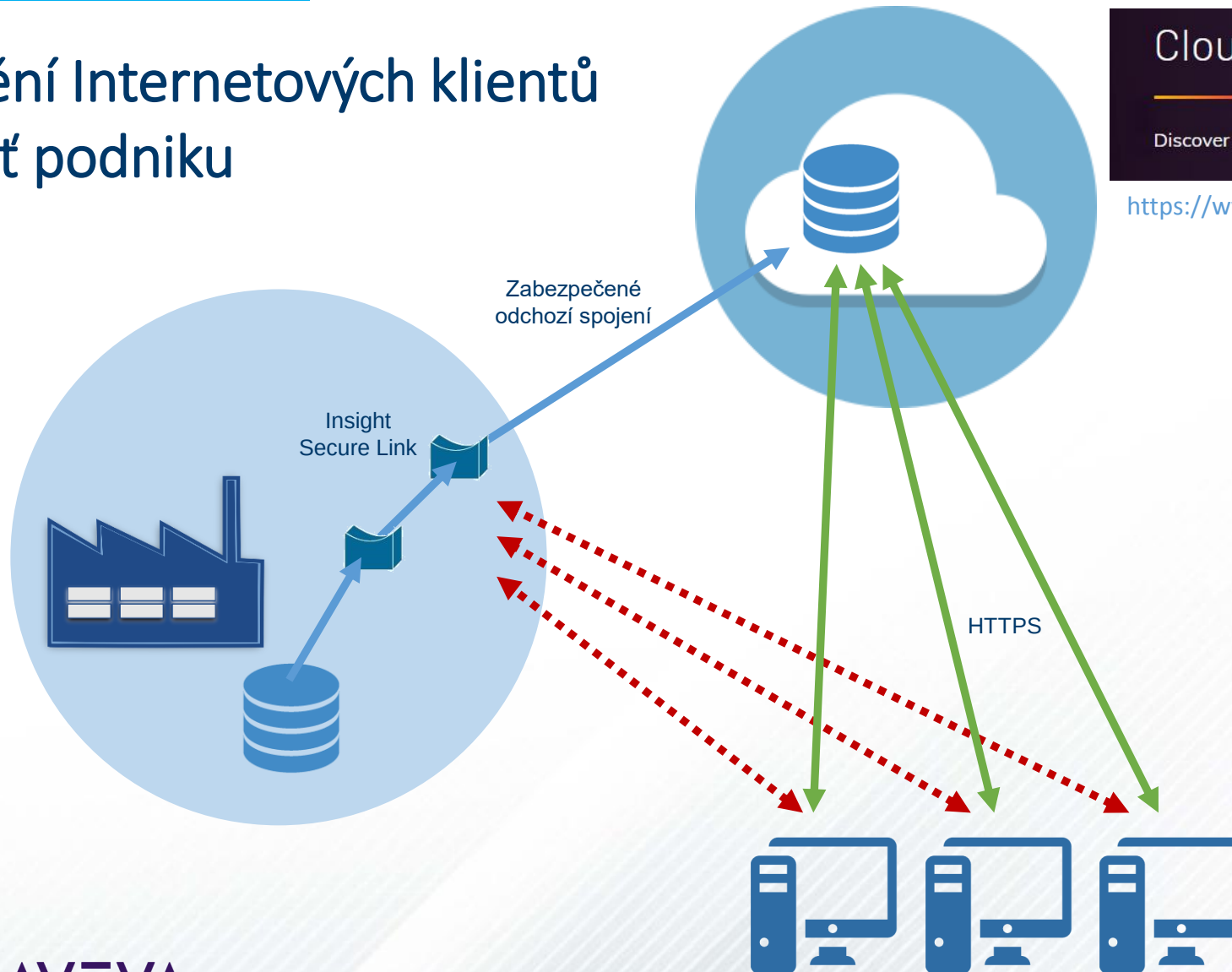
Address

Port:

[← Back](#) [Configure](#)

Význam cloudu ve strategii upevnění kybernetické bezpečnosti

- Odklonění Internetových klientů mimo síť podniku



Cloud Security Statement

Discover AVEVA's proactive stance on cybersecurity

<https://www.aveva.com/en/legal/trust/security/>

InTouch Web – konfigurace přístupu ze sítě mimo OT

The screenshot displays the AVEVA Application Manager interface. The 'Tools' menu is highlighted with a blue arrow, and a text label 'AIM = AVEVA Identity Manager' points to the 'WEB CLIENT' tab. The 'Web Client Settings' panel on the left shows various configuration options, including 'Graphic Refresh Rate (ms): 1000', 'Alarm Refresh Rate (ms): 1000', 'Web Client Site Name: InTouchWeb', 'Show Header: [checked]', 'Enable NavBar: [checked]', and 'Allow Anonymous Access: [unchecked]'. The 'AIM Registration' panel is open, showing 'Identity Server Settings'. A note states: 'Note: Please enter the administrator credentials of the Identity Server.' The 'Use AIM Server as the authentication server' checkbox is checked. The 'Identity Server' is set to 'win-vd56fub3sf5'. The 'User Name' field is labeled 'Enter user name', and the 'Password' field is labeled 'Enter password'. The 'Secure Gateway' is set to 'nginx.pantek.cz'. A red arrow points from the 'Secure Gateway' field to the 'Configurator' window. The 'Configurator' window shows a list of components on the left, including 'AVEVA Enterprise Licensing Platform', 'AVEVA Enterprise License', 'AVEVA Historian', 'Server', 'Security', 'Search', 'Reporting', 'AVEVA System Monitor', 'System Monitor Manager', 'Alert Email Server', 'AVEVA System Platform', 'Galaxy License Mode', 'Common Platform', 'System Management Server', 'Industrial Graphics Server', 'Client Settings', and 'Authentication Settings'. The 'User Authentication' option is selected and highlighted with a red box. A text label 'Reverzní proxy v DMZ' with a blue arrow points to the 'Secure Gateway' field in the 'Configurator' window. The 'Secure Gateway' field is labeled 'Secure Gateway' and contains the value 'nginx.pantek.cz'. Below the field, there is a description: 'The secure reverse proxy server installed in DMZ to allow Industrial Graphics Web Server to be accessed outside the plant network. Industrial Graphics Web Server can be used with a secure gateway only if registered with AVEVA Identity Manager.'

AVEVA Application Manager

File View Tools Help

INTOUCH OMI WEB CLIENT

Web Client Settings

Graphic Refresh Rate (ms): 1000

Alarm Refresh Rate (ms): 1000

Web Client Site Name: InTouchWeb

Show Header: [checked]

Enable NavBar: [checked]

Allow Anonymous Access: [unchecked]

AIM Registration

Identity Server Settings

Note: Please enter the administrator credentials of the Identity Server.

☒ Use AIM Server as the authentication server

Identity Server: win-vd56fub3sf5

User Name: Enter user name

Password: Enter password

Secure Gateway: nginx.pantek.cz

☒ Allow Industrial Graphics to connect to the Identity Server

Configurator

File Help

AVEVA Enterprise Licensing Platform

AVEVA Enterprise License

AVEVA Historian

Server

Security

Search

Reporting

AVEVA System Monitor

System Monitor Manager

Alert Email Server

AVEVA System Platform

Galaxy License Mode

Common Platform

System Management Server

Industrial Graphics Server

Client Settings

Authentication Settings

By default Web Client uses Windows Authentication. You can switch to user authentication in this configuration screen.

☒ User Authentication

You need to connect to a System Management Server to use this option.

AVEVA Identity Manager win-vd56fub3sf5:443

Secure Gateway nginx.pantek.cz

The secure reverse proxy server installed in DMZ to allow Industrial Graphics Web Server to be accessed outside the plant network. Industrial Graphics Web Server can be used with a secure gateway only if registered with AVEVA Identity Manager.

☐ Windows Authentication

Reverzní proxy v DMZ

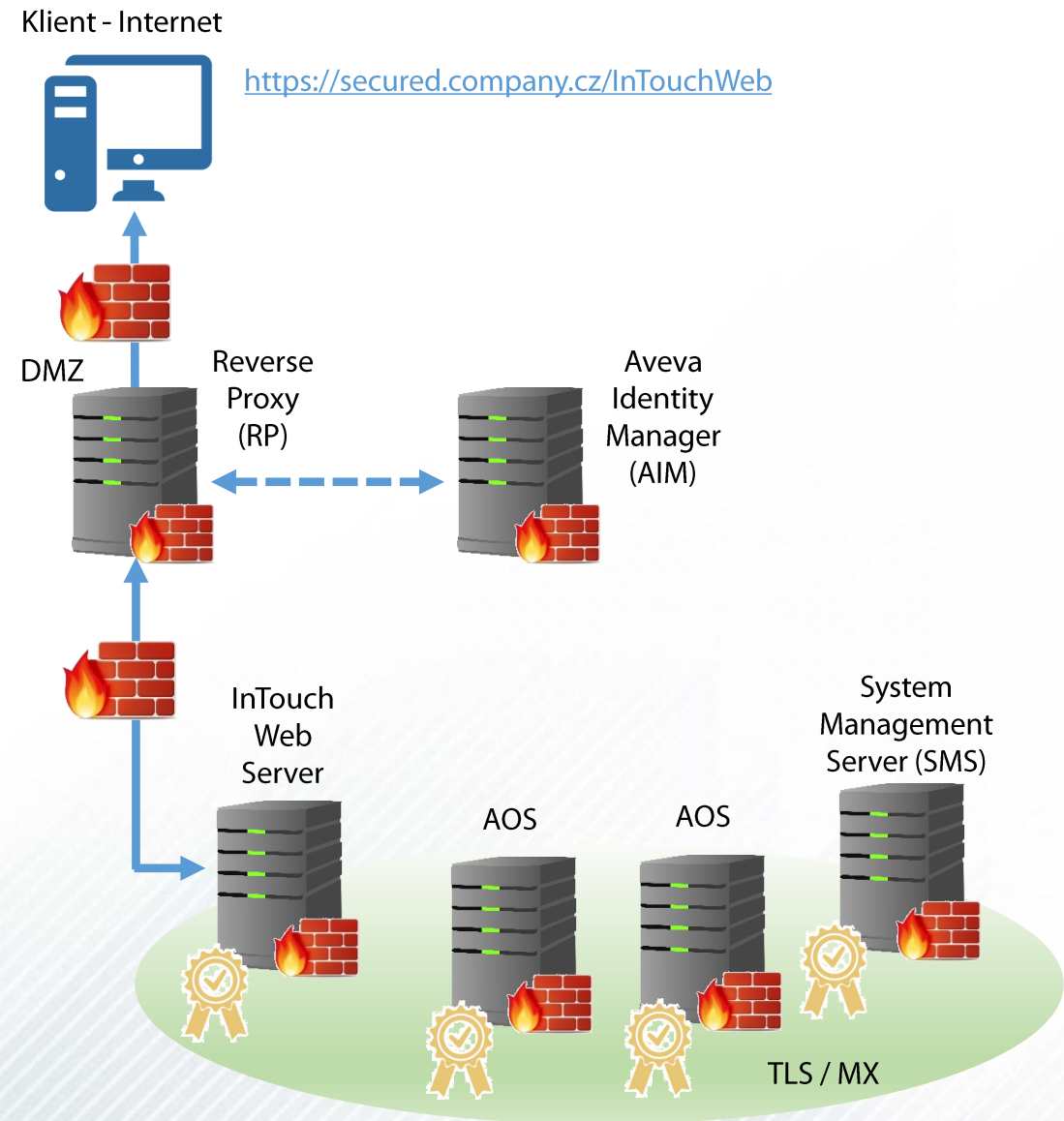
AIM, Reverzní Proxy, InTouch Web Server, SMS

▶ Reverzní Proxy

- ▶ Ověřuje uživatele na AIM
- ▶ Uživatel OK
 - ▶ Token zaslán na InTouch Web Server
 - ▶ Provoz přesměrován tamtéž

▶ InTouch Web Server

- ▶ Certifikován na SMS
 - ▶ Poskytuje web pouze přes HTTPS
 - ▶ Posílá na Reverse Proxy
 - ▶ Může komunikovat data z platformy
 - ▶ MX šifrováno
 - ▶ Uzly se „znají“



| Ubránitelný systém

Shrnutí a doplnění

Ubránitelný ICS se SW AVEVA

- ▶ **4xA až na úroveň datového bodu**
- ▶ **Nepodcenit audit řídicího systému**
 - ▶ Např. přehrání programu v PLC je z hlediska CS významná/závažná událost!
- ▶ **Šifrovaná komunikace mezi autentickými uzly systému**
 - ▶ Pozor na otevřené protokoly!
- ▶ **Segmentace sítě, firewally/porty, DMZ, jasně definované datové toky**
 - ▶ Jediná brána do kritické části systému, DMZ aplikace
 - ▶ Zákaz přímého provozu kancelářských služeb (mail/web...) v procesní síti (lze zprostředkovat z IT sítě)
- ▶ **Ochrana koncových systémů (end-point security)**
 - ▶ Aktualizace systémů (podporované OS, KB/CS záplaty), viz. AVEVA Security Central
- ▶ **Krizové plány**
 - ▶ Reakce na útok, zachování kontinuity a zabezpečení kritických funkcí, rychlá obnova
 - ▶ Možnost izolovat (uzel, síť) a eliminovat (uživatelé)

Doplnění: Produkty z našeho portfolia pro upevnění CS

▶ Versiondog

- ▶ Audit změn programů v PLC

▶ ThinManager

- ▶ Minimalizace napadnutelných systémů v procesní síti
 - ▶ Tenká koncová pracoviště bez možnosti interakce s hostitelským OS
 - ▶ Na zero klientech zcela chybí brány, přes které může vstupovat malware
- ▶ Management přihlašovacích údajů pro relace VP
 - ▶ Operátor nezná přihlašovací údaje pro otevření relací VP => nemůže je vyrazit ani zneužít
 - ▶ Naplnění politiky hesel Active Directory (expirace, komplexita)
- ▶ Upevnění CS - vícefázové přihlášení
 - ▶ Biometrika, Smart ID, RFID, PINy,...

| Děkuji za pozornost

Otázky, odpovědi



Váš partner ve světě digitální transformace

Sušilova 1528/1
500 02 Hradec Králové
Česká republika

www.pantek.cz