Kapitola 1 - Příloha 2 – ATEAS API

1.1. ATEAS API pro kamerové servery (ATEAS Server)

1.1.1. Princip komunikace

Kamerové servery mohou události přijímat pomocí protokolu TCP/IP na specifickém událostním portu 8505 (viz příloha Konfigurace sítě). Data jsou v textové podobě a pro komunikační kanál lze nastavit kódování textu, implicitně se používá kódování ASCII, lze však zvolit také kódování UNICODE, UTF8, Windows 1250 či další.

Princip komunikace po síti s využitím protokolu TCP/IP: Při předání příkazu ATEAS API musí vždy strana generující příkaz vytvořit TCP/IP spojení ke kamerovému serveru. V rámci jednoho vytvořeného TCP spojení lze zasílat více příkazů, stejně jako je možné pro každý příkaz vytvořit nové spojení. Kamerový server akceptuje nejvýše 50 současných připojení na vstupní port pro příjem příkazů ATEAS API. Pokud tedy budou příkazy generovány z více než 50 zdrojů (např. ze všech kamer připojených ke kamerovému serveru – až 999), musí být neaktivní spojení uzavírána.

Obecná syntaxe: Veškeré příkazy ATEAS API jsou v hranatých závorkách, data mimo hranaté závorky nejsou vyhodnocována. Protokol nerozlišuje velká a malá písmena.

1.1.2. Příjem externích událostí

Systém ATEAS Security obsahuje stále se rozšiřující počet možných zdrojů událostí, které mohou synchronizovat celý kamerový systém. Např. detekce pohybu, výpadek kamery nebo (de)aktivace poplachového vstupu mohou na jednom či více kamerových serverech a na jedné či více kamerách zároveň vyvolat různé reakce dle nastavení událostního scénáře (zahájení záznamu či zvýšení záznamové snímkové frekvence, aktivace poplachových výstupů, přepnutí definovaného pohledu kamer na monitor definovaných uživatelů, natočení kamery, odeslání notifikací (e-mail) apod.

Vývoj v oblasti inteligentního videa umožňuje do koncových kamerových bodů nahrát aplikace představující specifické zdroje událostí, integrační tendence dále vyžadují, aby kamerový systém reagoval na ostatní systémy (systém kontroly vstupu, PCO a mnohé další). Z libovolného z těchto systémů je možné vyvolat libovolné reakce kamerového systému pomocí programového rozhraní ATEAS API.

Obecný tvar textové zprávy je následující:

[ATEAS EVENT {START,STOP} kamera kódové_jméno data]

kde

(kamera) udává číslo kamery na daném kamerovém serveru (musí být v rozsahu 1 až maximální možné číslo kamery na daném serveru - 999),
(kódové jméno) je registrované kódové označení administrátorem definované vlastní události kamer v části administrace kamer – vlastní události,
(data) mohou obsahovat libovolnou textovou informaci, která bude uložena spolu s událostí a do databáze metadat. Limit pro délku je 200 znaků. Položka data je nepovinná a nemusí být obsahem zprávy.

Příklady:

[ATEAS EVENT START 2 TAMPER]
[ATEAS EVENT STOP 2 TAMPER]
[ATEAS EVENT START 2 AUDIO]
[ATEAS EVENT START 1 CARWEIGHT 1500kg]

POZNÁMKA

Pokud událost není nebo nemůže být ukončena příkazem STOP, je s ní zacházeno stejně jako s interní událostí dle nastavení událostních parametrů (tj. může být ukončena automaticky).

Příklad užití:

Detekci zvuku či např. sabotáž kamery (Active Tampering Alarm) lze u Axis kamer připojit pomocí webového rozhraní příslušné kamery vytvořením událostního serveru TCP (nastavení na IP adresu kamerového serveru a jeho událostní port 8505) v části Event Servers (případně Events - Recipients) a vytvořením události v části Event Types (případně Events - Action Rules) s napojením na vytvořený TCP server a se zprávou dle požadavků ATEAS API.

1.1.3. Vkládání metadat

Pro vložení metadat ke kamerovému serveru pro možnost video synchronizace je možné využít nejen zprávy o události, ale také přímé vložení metadat. Při přímém vložení metadat nebude v systému vyvolána událost.

[ATEAS META kamera čas kódové_jméno data]

kde

(kamera) udává číslo kamery na daném kamerovém serveru,
(čas) je číselný údaj reprezentující časové razítko, nulová hodnota znamená, že čas bude určen serverem, pozitivní hodnota je vyhodnocena jako absolutní čas v UTC vyjádřený v počtu 100-nanovteřinových intervalů od 1.1.1601, negativní hodnota je interpretována jako posun oproti současnému času serveru směrem do minulosti vyjádřený v milivteřinách,
(kódové jméno) je registrované kódové označení administrátorem definované vlastní události kamer v části administrace kamer – vlastní události,
(data) mohou obsahovat libovolnou textovou informaci, která bude uložena do databáze metadat. Limit pro délku je 200 znaků. Položka data je nepovinná a nemusí být obsahem zprávy.

Příklady:

[ATEAS META 1 0 SCAN AB512459]
[ATEAS META 2 -1000 SCAN AC548947]
[ATEAS META 3 132125472000000000 SCAN AC548947]

POZNÁMKA

Při posunu času není akceptován posun větší než 30 dní směrem do minulosti a 1 minutu směrem do budoucnosti.

POZNÁMKA

Posuny času jsou vhodné v případě, že externí data jsou do systému doplněna offline anebo není možné je zasílat přesně v reálném čase.

1.2. ATEAS API pro administrační server (ATEAS Administrator)

1.2.1. Princip komunikace

Administrační server může události přijímat na specifickém událostním portu 8504 (viz příloha Konfigurace sítě) a také přes sériové porty COM1 či COM2. Data jsou v textové podobě a pro

komunikační kanály lze nastavit kódování textu, implicitně se používá kódování ASCII, lze však zvolit také kódování UNICODE, UTF8, Windows 1250 či další.

Princip komunikace po síti s využitím protokolu TCP/IP: Při předání příkazu ATEAS API musí vždy strana generující příkaz vytvořit TCP/IP spojení k administračnímu serveru. V rámci jednoho vytvořeného TCP spojení lze zasílat více příkazů, stejně jako je možné pro každý příkaz vytvořit nové spojení. Administrační server akceptuje nejvýše 50 současných připojení na vstupní port pro příjem příkazů ATEAS API. Pokud tedy budou příkazy generovány z více než 50 zdrojů, musí být neaktivní spojení uzavírána.

Princip komunikace pomocí sériového portu: Pro předání příkazu pomocí sériové spojení na port COM1 či COM2, musí strana generující příkaz otevřít příslušný sériový port se stejnými parametry, jaké budou nastaveny v ATEAS Security. Jedná se zejména o přenosovou rychlost, paritu, počet datových bitů a počet stopbitů.

Obecná syntaxe: Veškeré příkazy ATEAS API jsou v hranatých závorkách, data mimo hranaté závorky nejsou vyhodnocována. Protokol nerozlišuje velká a malá písmena.

1.2.2. Příjem externích událostí

Obecný tvar zprávy je následující:

[ATEAS EVENT {START,STOP} objekt id]

kde

(objekt) je numerická hodnota v rozsahu 1 až 10 000, která je hlavním kódem identifikujícím událost – např. číslo zastřeženého objektu,
(id) je numerická hodnota v rozsahu 1 až 99 999, která je vedlejším kódem identifikujícím událost – např. číslo smyčky v zastřeženém objektu.

Příklady:

[ATEAS EVENT START 1 1]
[ATEAS EVENT STOP 1 1]
[ATEAS EVENT START 100 2]
[ATEAS EVENT START 150 60]

Příklad užití:

Pult centrální ochrany (PCO) firmy NAM lze doplnit o modul SERVIS COM, který posílá události systému pomocí sériového spojení. Tvar informací je konfigurovatelný a lze tudíž nastavit do očekávaného tvaru v souladu s ATEAS API. V systému ATEAS Security postačí správně nastavit parametry sériového spojení, vytvořit událostní scénáře a ty přiřadit jednotlivým objektům a smyčkám.

1.2.3. Ovládání video stěny

Obecný tvar zprávy je následující:

[ATEAS VIDEOWALL monitor (submonitor = 0) {serverid | 0} {deviceid | urlid} (wallid = 1) (meta = 0)]

kde

(monitor) je numerická hodnota v rozsahu 1 až 192, která udává číslo monitoru na fyzické či virtuální video stěně,
(submonitor) je numerická hodnota v rozsahu 0 až 16, která udává číslo submonitoru při použití monitorů typu Quad, Triple, nebo Šestnáct.
(serverid) je numerická hodnota v rozsahu 0 – 9 999, která identifikuje kamerový server,
(deviceid) je numerická hodnota v rozsahu 0 – 999, která udává číslo kamery na příslušném serveru,
(urlid) je numerická hodnota v rozsahu 1 – 9 999, která udává číslo URL (pokud je serverid 0),
(wallid) je numerická hodnota v rozsahu 1 – 1000, která udává číslo video stěny v systému,
(meta) je numerická hodnota 0 nebo 1 pro zobrazení metadat na video stěně.

Příklady:

[ATEAS VIDEOWALL 1 1 3]
[ATEAS VIDEOWALL 2 1 4]
[ATEAS VIDEOWALL 3 1 1 4]

POZNÁMKA

Jsou-li obě hodnoty serverid a deviceid rovny nule, dojde k vypnutí příslušného monitoru (vypnutí videa a přechod do výchozí podoby s logem ATEAS).

POZNÁMKA

Hodnota (submonitor) je z důvodu kompatibility nepovinná s implicitní hodnotou 0. Pokud je prováděno přepnutí na monitor typu Standard nebo Poplach, musí být hodnota 0 (pokud je uvedena). Na monitor typu Quad musí být přepnutí provedeno s hodnotou submonitor 1, 2, 3, nebo 4 apod.

POZNÁMKA

Na video stěnu lze při událostech přepínat monitory též automaticky (bez použití ATEAS API), pokud jsou některé monitory zařazeny do skupiny událostních monitorů. Více viz kapitoly o video stěně.

POZNÁMKA

Hodnota wallid je nepovinná a pokud není zadána, použije se hodnota jedna, což je číslo hlavní dopředu vytvořené video stěny. Když chceme číslo video stěny do zprávy doplnit, musíme zároveň zadat i hodnotu pro submonitor, jinak by nebylo možné zprávu správně vyhodnotit.

Pokud je serverid nastaveno na hodnotu nula, je pozitivní deviceid interpretováno jako ID pro URL vložené do systému administrátorem.

Příklad užití: Pomocí libovolné externí aplikace lze na virtuální či fyzickou video stěnu provádět přepínání kamer z libovolného serveru.

1.2.4. Zasílání informací o událostech

POZOR

Události jsou zasílány pouze pomocí komunikačního kanálu TCP/IP. Nelze tedy přijímat informace o událostech např. pomocí sériového spojení.

Po navázání TCPIP spojení se zohledněním informací předchozích subkapitol jsou po tomto komunikačním kanále zasílány informace o událostech v systému. Zasílány jsou veškeré události vyvolané činností kamer včetně detekce pohybu, aktivace poplachových vstupů, výpadku kamer,

vlastních událostí kamer či detekce RZ. Přes toto jediné spojení s administračním serverem systému jsou zasílány události ze všech kamerových serverů nezávisle na jejich umístění.

Jednotlivé události jsou zasílány se všemi podstatnými náležitostmi v podobě krátkých XML dokumentů.

Zahájení události

Základní podoba XML dokumentu, který je vygenerován a zaslán pomocí TCPIP spojení v případě výskytu události, je následující:

```
<?xml version="1.0" encoding="utf-8"?>
<ateas>
	<event>
		<id>ID</id>
		<imageid>ID snímků</imageid>
		<level>Úroveň</level>
		<server>
			<id>ID serveru</id>
			<name>Název serveru</name>
		</server>
		<camera>
			<id>ID kamery</id>
			<name>Název kamery</name>
		</camera>
		<source>
			<id>ID zdroje</id>
		</source>
		<datetime>
			<utcstamp>Časové razítko</utcstamp>
			<localvalue>Datum a čas</localvalue>
		</datetime>
		<data>Data</data>
		<dataex>Data 2</dataex>
		<uuid>UUID</uuid>
		<videoobject>
			<rectangle>Pozice</rectangle>
		</videoobject>
	</event>
```

```
</ateas>
```

Ukončení události

```
<?xml version="1.0" encoding="utf-8"?>
<ateas>
      <eventstop>
            <id>ID</id>
            <datetime>
                  <utcstamp>Časové razítko</utcstamp>
                  <localvalue>Datum a čas</localvalue>
            </datetime>
            <data>Data</data>
      </eventstop>
</ateas>
```

Význam jednotlivých hodnot uvnitř XML značek je následující:

ID – Jednoznačný identifikátor události (vzestupně od čísla 1 od startu serveru).

ID snímků – Identifikátor, který jednoznačně váže XML notifikace k exportovaným snímkům pomocí protokolu FTP. Toto ID je úvodní součástí názvu exportovaného souboru.

Level – Stupeň závažnosti události, systém rozlišuje dle nastavení časových plánů běžnou událost (1) a poplach (2).

ID serveru – Identifikace serveru, např. 1, 2. Pro edice HOME a PROFESSIONAL vždy 1.

Název serveru – Název serveru, např. Server 1.

ID kamery – Identifikace kamery, např. 1, 2.

Název kamery – Název kamery, např. Kamera 1.

ID zdroje – Identifikace zdroje události. Viz seznam níže.

Časové razítko – Absolutní čas výskytu události vyjádřený jako počet 100 nanosekundových intervalů uplynulých od půlnoci 1. ledna 1601 UTC. Údaj je tudíž očištěn od vlivů časového pásma a změn letního času, např. 128989433710312500.

Datum a čas – Formátovaný údaj o datu a času události se zohledněním časového pásma a změn letního času ve formátu d.M.yyyy H:mm:ss, např. 9.10.2009 9:05:51.

Data – Data události, může být použito pro rozšiřující data o události např. RZ vozidel – 2A5 6217, AEP 44-44.

Data 2 – Dodatečná data události podle jejího typu.

UUID – Dodatečný identifikátor zdroje události (pokud je k dispozici), který může blíže identifikovat zdroj.

Pozice – Udává pozici objektu v obraze ve formátu X Y W H, kde X Y jsou souřadnice pozice objektu a W a H udávají jeho šířku a výšku. Všechny údaje jsou uvedeny v absolutních souřadnicích pro velikost přidruženého snímku.

Pro posouzení události z hlediska děje, který ji vyvolal, je rozhodující hodnota ID zdroje. Tato hodnota vyjadřuje zdroj události, tedy skutečnost, která vedla ke vzniku události na příslušné kameře.
V současnosti se pomocí ATEAS API rozlišují a zasílají následující hodnoty označení zdroje události:

1 – detekce pohybu na kameře, data jsou prázdná
2 – výpadek kamery, data jsou prázdná
3 – aktivace poplachového vstupu kamery, data obsahují číslo vstupu (1, 2, 3, 4, …)

10 – rozpoznání RZ vozidla – neregistrovaná, data obsahují RZ vozidla v dekorativním tvaru
11 – rozpoznání RZ vozidla – povolená, data obsahují RZ vozidla v dekorativním tvaru
12 – rozpoznání RZ vozidla – zakázaná, data obsahují RZ vozidla v dekorativním tvaru
13 – rozpoznání RZ vozidla – uživatelská 1, data obsahují RZ vozidla v dekorativním tvaru
14 – rozpoznání RZ vozidla – uživatelská 2, data obsahují RZ vozidla v dekorativním tvaru

20 – analytická událost – narušení, data jsou prázdná
21 – analytická událost – překonání čáry, data jsou prázdná
22 – analytická událost – překonání překážky, data jsou prázdná
23 – analytická událost – odložený předmět, data jsou prázdná
24 – analytická událost – odebraný předmět, data jsou prázdná
25 – analytická událost – zastavení vozidla, data jsou prázdná
26 – analytická událost – podezřelý pohyb, data jsou prázdná
27 – analytická událost – posun kamery, data jsou prázdná
28 – analytická událost – ztráta videosignálu, data jsou prázdná

29 – analytická událost – sledování objektu, data jsou prázdná
30 – analytická událost – špatný signál, data jsou prázdná
31 – analytická událost – detekce obličeje, data jsou prázdná

32 – kontrola kvality videa, data obsahují požadovanou úroveň snímkové frekvence

40 – detekce pohybu na serveru, data jsou prázdná

51 – 100 – vlastní události kamer definované administrátorem, lze využít pro libovolné typy událostí, např. sabotáž kamery, detekce zvuku a další, data mohou obsahovat uživatelská data zdroje události

110 – událost ručního nahrávání kamery, data jsou prázdná

111 – 130 – Onvif zdroje událostí, data mohou obsahovat Onvif data zdroje události

131 – 150 – komplexní zdroje událostí vytvořené administrátorem a složené z jiných elementárních událostních zdrojů, data jsou prázdná

151 – 200 – vlastní události kamer definované administrátorem, lze využít pro libovolné typy událostí, např. sabotáž kamery, detekce zvuku a další, data mohou obsahovat uživatelská data zdroje události

201 – 250 – analytické události definované administrátorem vyhodnocované moduly neuronové sítě na kamerovém serveru

POZNÁMKA

Aby mohly události kamer vzniknout a mohly být zasílány v rámci ATEAS API do všech vytvořených TCPIP spojení, musí být příslušné zdroje událostí staticky nebo dynamicky časově mapovány, volitelně může být definován událostní scénář. Viz kapitoly o událostním řízení.

POZNÁMKA

Aby bylo možné provést TCP připojení pro komunikaci pomocí ATEAS API, je třeba zajistit dostupnost příslušného síťového portu v aplikaci ATEAS Administrator uvedeného v příloze dokumentace.

POZNÁMKA

Pro zajištění bezpečnosti je možné v systému ATEAS Security pomocí nástroje IP filtrace určit adresy, ze kterých bude povoleno připojení komunikačního kanálu ATEAS API.

POZNÁMKA

Součástí XML dokumentu mohou být též znaky s diakritikou nebo specifické znaky jiných jazyků (např. v názvu kamery), v takovém případě je nutné dbát na nastavení kódování textu při otevírání TCP kanálu pomocí klienta ATEAS Observer. Kromě XML dokumentů může server zasílat také keep-alive byty s hodnotou 0, znaky vně XML dokumentů však není nutné nijak zohledňovat.

POZOR

ID události je jednoznačný identifikátor, pomocí kterého jsou události číslovány vzestupně od čísla 1 od startu administračního serveru. Restart administračního serveru tedy provede reset čísla zpět na hodnotu 1 a může také způsobit, že některé události nejsou ukončeny.

1.2.5. Uživatelské funkce

Pomocí zpráv ze skupiny uživatelského managementu je možné získat informaci o tom, že se uživatel úspěšně přihlásil do systému nebo ho opustil. Jiný typ zpráv naopak dovede provést nucené odhlášení uživatele, pokud je do systému přihlášen.

POZNÁMKA

Pomocí této skupiny zpráv je možné např. jednoduchou integrací s docházkovým systémem zajistit či kontrolovat, zdali uživatel vstupuje do systému oprávněně či zdali se nejedná o zneužití uživatelského účtu jinou osobou.

Při přihlášení či odhlášení uživatele dojde k zaslání této informace v podobě jednoduchého XML dokumentu s následujícím tvarem.

```
<?xml version=”1.0” encoding=”utf-8”?>
```

```
<ateas>
      <user>
            <id>ID</id>
            <name>Uživatelské jméno</level>
            <action>Akce</action>
            <datetime>
                  <utcstamp>Časové razítko</utcstamp>
                  <localvalue>Datum a čas</localvalue>
            </datetime>
      </user>
</ateas>
```

Význam jednotlivých hodnot uvnitř XML značek je následující:

ID – Jednoznačný identifikátor uživatele, např. 20.

Uživatelské jméno – Jméno uživatele dle hodnoty v systému.

Akce – Hodnota logon (při přihlášení) nebo logout (při odhlášení).

Časové razítko – Absolutní čas výskytu události vyjádřený jako počet 100 nanosekundových intervalů uplynulých od půlnoci 1. ledna 1601 UTC. Údaj je tudíž očištěn od vlivů časového pásma a změn letního času, např. 128989433710312500.

Datum a čas – Formátovaný údaj o datu a času události se zohledněním časového pásma a změn letního času ve formátu d.M.yyyy H:mm:ss, např. 9.10.2009 9:05:51.

1.3. Parametrické spouštění aplikací

Aplikace ATEAS Security je možné spouštět také s dodatečnými parametry, které jsou předány spustitelnému souboru při startu aplikace či služby. Přidání těchto parametrů je možné v nastavení služby v systému Windows. V současné době existují parametry popsané níže.

1.3.1. Administrační server

Parametr	Hodnoty	Význam	Poznámka
-ssl	heslo	Heslo certifikátu	Je nutné zadat, pokud je použitý certifikát ve formátu PFX chráněn heslem.

1.3.2. Kamerový server

Parametr	Hodnoty	Význam	Poznámka
-ssl	heslo	Heslo certifikátu	Je nutné zadat, pokud je použitý certifikát ve formátu PFX chráněn heslem.
-loglevel	0 - 1	Nastavení úrovně logování	Pozitivní hodnota zapíná výpis zaplnění vyrovnávací paměti serveru do podsložky log.