

Výkonné jádro systému REXYGEN

Uživatelská příručka

REX Controls s.r.o.

Verze 3.0
15.12.2023
Plzeň

Obsah

1	Úvod	2
2	Konfigurace	3
2.1	Umístění konfiguračních souborů	3
2.2	Popis nastavení konfigurace	4
3	Záznam systému	7
3.1	Zdroje a závažnosti	7
4	Webové rozhraní	8
4.1	Dostupné služby	8
5	Autentizace	9
5.1	Uživatelé a role	9
5.2	Užití unixových účtů	10
6	Zabezpečení	11
	Literatura	13

Kapitola 1

Úvod

Nejdůležitější součástí systému REXYGEN je jádro obsažené v softwarové komponentě zvané RexCore. RexCore je v případě operačních systémů *Windows* a *GNU/Linux* nezávislý proces, v případě hard real-time operačního systému se jedná o skupinu úloh v reálném čase, anebo je to, v případě mikrokontroléru, celý systém. V každém případě jde o komponentu, kde běží řídicí algoritmus vyvinutý uživatelem. RexCore ovládá periferie zařízení, na kterém pracuje a s jeho pomocí se iniciuje komunikace s ostatními zařízeními, která se podílejí na řídicím procesu. Zároveň poskytuje detailní diagnostiku různých komunikačních protokolů pro uživatelské rozhraní.

Tento dokument obsahuje veškeré informace sloužící ke konfiguraci softwarové komponenty RexCore na operačních systémech Windows a GNU/Linux, které jsou potřebné ke správnému běhu. Vývojář řídicího algoritmu by si měl přečíst [1]. Uživatel, který zatím není obeznámen se systémem REXYGEN by si měl přečíst jakýkoli z manuálů pro začátečníky, např. [2], [3], [4].

Nutno poznamenat, že přestože bylo vynaloženo mnoho úsilí na sjednocení komponenty RexCore na všech podporovaných platformách, je nemožné poskytnout naprosto identickou funkcionalitu a výkon na všech zařízeních. Uživatel by měl volit cílovou platformu opatrně a případně zkontaktovat požadavky se společností REX Controls.

Kapitola 2

Konfigurace

Samotné jádro RexCore vyžaduje pouze minimální interakci s uživatelem. Ve skutečnosti není interakce nutná vůbec ve chvíli, kdy proběhne standardní instalace nebo je použit standardní distribuční kanál a výchozí konfigurace je pro uživatele postačující. Občas je však nutné výchozí konfiguraci upravit nebo zabezpečit řídicí systém při uvedení do provozu a někdy i během vývoje.

2.1 Umístění konfiguračních souborů

Všechny soubory důležité pro správné fungování komponenty RexCore jsou umístěny v *konfiguračním adresáři*. *Konfigurační adresář* je umístě `/rex/rexcore` v případě GNU/Linux a v adresáři `C:\ProgramData\REX Controls\REX<verze>\RexCore` v případě systému Windows.

V *konfiguračním adresáři* mohou být přítomny tyto soubory:

- `license.txt` – Soubor obsahující licenční klíče pro zařízení. Může být uživatelem umístěn manuálně, ale použití nástrojů REXYGEN Studio nebo REXYGEN DWM pro licenční operace je nejobvyklejší.
- `exec.rex` – Binární soubor obsahující konfiguraci řídicího algoritmu. Uživatel by neměl manipulovat s tímto souborem, aniž by věděl, co dělá.
- `hmi.rex` – Binární soubor obsahující konfiguraci rozhraní HMI. Uživatel by neměl manipulovat s tímto souborem, aniž by věděl, co dělá.
- `auth.rex` – Binární soubor obsahující konfiguraci uživatelů, skupin a oprávnění. Uživatel by neměl manipulovat s tímto souborem, aniž by věděl, co dělá.
- `rexcore.cfg` – Textový soubor pro jádro RexCore se všemi dostupnými a nastavitelnými možnostmi konfigurace. Podrobný popis nastavení je popsán v sekci 2.2.

2.2 Popis nastavení konfigurace

Konfigurace RexCore probíhá pomocí úpravy nastavení konfigurace v souboru `rexcore.cfg`. Každá jednotlivá možnost by měla být na samostatném řádku a měla by mít formát `možnost=hodnota` bez mezer nebo tabulátorů. Následující tabulka obsahuje popisy jednotlivých nastavení konfigurace.

Nastavení	Výchozí hodnota	Popis
<code>server.tcp</code>	<code>:43981</code>	Adresa a port na kterých by měl diagnostický subsystém jádra RexCore vyčkávat příchozí TCP spojení. Nastavte na "disabled" pro vypnutí této služby. Zástupná adresa se využívá ve chvíli, kdy adresa není specifikována, což znamená, že subsystém vyčkává na spojení u všech síťových rozhraní.
<code>server.ssl</code>	<code>:43997</code>	Adresa a port na kterých by měl diagnostický subsystém jádra RexCore vyčkávat příchozí SSL spojení. Nastavte na "disabled" pro vypnutí této služby. Zástupná adresa se využívá ve chvíli, kdy adresa není specifikována, což znamená, že subsystém vyčkává na spojení u všech síťových rozhraní.
<code>server.http</code>	<code>:8008</code>	Adresa a port na kterých by měl diagnostický subsystém jádra RexCore vyčkávat příchozí HTTP spojení. Nastavte na "disabled" pro vypnutí této služby. Zástupná adresa se využívá ve chvíli, kdy adresa není specifikována, což znamená, že subsystém vyčkává na spojení u všech síťových rozhraní.
<code>server.https</code>	<code>:8009</code>	Adresa a port na kterých by měl diagnostický subsystém jádra RexCore vyčkávat příchozí HTTPS spojení. Nastavte na "disabled" pro vypnutí této služby. Zástupná adresa se využívá ve chvíli, kdy adresa není specifikována, což znamená, že subsystém vyčkává na spojení u všech síťových rozhraní.
<code>auth.enabled</code>	<code>1</code>	Povolit/zakázat autentizační subsystém. Pokud je povoleno, uživatel musí být autentizován pomocí uživatelského jména a hesla. Pokud je zakázáno, autentizace není potřeba.

<code>auth.allowssystem</code>	1	Povoluje nebo zakazuje možnost přihlásit se do systému REXYGEN pomocí unixových účtů. Toto nastavení je dostupné pouze na zařízeních GNU/Linux. Viz sekci 5.2 pro více informací.
<code>auth.allowroot</code>	1	Povoluje nebo zakazuje možnost přihlásit se do systému REXYGEN jako <code>admin</code> pomocí unixového root účtů. Toto nastavení je dostupné pouze na zařízeních GNU/Linux. Viz sekci 5.2 pro více informací.
<code>auth.super.enabled</code>	0	Povoluje nebo zakazuje <i>super</i> účty. Viz sekci 5.1 pro více informací.
<code>auth.operator.enabled</code>	0	Povoluje nebo zakazuje <i>operator</i> účty. Viz sekci 5.1 pro více informací.
<code>auth.guest.enabled</code>	0	Povoluje nebo zakazuje <i>guest</i> účty. Viz sekci 5.1 pro více informací.
<code>log.file.enabled</code>	0	Povoluje nebo zakazuje zápis do souboru definovaného nastavením <code>log.file</code> .
<code>log.file</code>	<code>rexcore.log</code>	Záznamový soubor RexCore, kde jsou uloženy veškeré diagnostické zprávy ze systémového logu, pokud je nastavení <code>log.file.enabled</code> povoleno.
<code>hmi.file</code>	<code>hmi.rex</code>	Soubor HMI
<code>auth.file</code>	<code>auth.rex</code>	Soubor autentizační databáze
<code>exec.file</code>	<code>exec.rex</code>	Konfigurační soubor algoritmu
<code>hmi.path</code>	<code>../www/hmi</code>	Cesta pro přidané/statické HMI soubory. Cesta je absolutní nebo relativní vůči konfiguračnímu adresáři RexCore.
<code>archive.path</code>	<code>../arc</code>	Cesta pro binární soubory s archivními daty. Cesta je absolutní nebo relativní vůči konfiguračnímu adresáři RexCore.
<code>data.path</code>	<code>../data</code>	Cesta pro datové soubory bloků a ovladačů. Cesta je absolutní nebo relativní vůči konfiguračnímu adresáři RexCore.
<code>web.webroot</code>	<code>../www</code>	Cesta kořenu dokumentu statických webových souborů, které setrvávají na cílovém zařízení. Cesta je absolutní nebo relativní vůči konfiguračnímu adresáři RexCore.
<code>perm.file</code>	<code>permem.dat</code>	Soubor trvalé paměti
<code>perm.file.size</code>	10240	Velikost souboru trvalé paměti
<code>perm.file.period</code>	300	Perioda ukládání souboru trvalé paměti

<code>rexcore.cert</code>	<code>rexcore.cer</code>	Soubor certifikátu RexCore využívaný pro HTTP nebo diagnostické připojení přes SSL. Soubor by měl být ve formátu PEM.
<code>rexcore.privkey</code>	<code>texttrexcore.key</code>	Soubor privátního klíče RexCore využívaný pro HTTP nebo diagnostické připojení přes SSL. Soubor by měl být ve formátu PEM.
<code>dgn.messages</code>	<code>0xc333370</code>	Diagnostické zprávy zobrazené v systémovém logu. Uživatel by neměl toto nastavení upravovat přímo, ale měl by použít program REXYGEN Studio ke konfiguraci systémového logu. Viz kapitolu 3 pro více informací.

Kapitola 3

Záznam systému

Jádro RexCore má vestavěný záznam systému (log), kde se shromažďují veškeré diagnostické zprávy. Mezi ně patří chyby, varování a informační zprávy, které mohou mít dopad na konání řídicího algoritmu.

Každá zpráva, která je do záznamu systému zapsána, obsahuje informaci a datu a času zápisu a parametry indikující zdrojový subsystém a závažnost zprávy.

3.1 Zdroje a závažnosti

V systému REXYGEN existují následující zdroje diagnostických zpráv:

- OS - abstraktní vrstva operačního systému,
- CORE - jádro,
- DIAG - diagnostický subsystém,
- BLOCK - algoritmy funkčních bloků,
- IODRV - vstup/výstup komunikačních ovladačů.

Rozlišují se následující závažnosti:

- Error (chyba),
- Warning (varování),
- Information (informace),
- Verbose information (podrobná informace).

Viz [5] pro více informací o možnostech konfigurace záznamu systému.

Kapitola 4

Webové rozhraní

Počínaje verzí 2.50 systému REXYGEN, je vestavěný přímo do subsystému RexCore vysoce optimalizovaný webový server. Server při výchozím nastavení vyčkává na HTTP připojení na portu 8008 a na HTTPS připojení na portu 8009. Pro možnost využívat HTTPS připojení je nutná instalace certifikátu a privátního klíče. Viz kapitolu 6 pro více informací.

4.1 Dostupné služby

Následující služby jsou zpracovávány vestavěným webovým serverem:

- odesílání obsahu statických souborů z konfiguračních souborů exekutivy,
- odesílání obsahu statických souborů z adresáře specifikovaného konfiguračním nastavením `web.webroot`,
- poskytování dynamického obsahu přes REST API,
- poskytování dynamického obsahu přes připojení přes protokol WebSocket,
- zpracování diagnostických připojení přes protokol WebSocket.

Viz [6] a [7] pro více informací.

Kapitola 5

Autentizace

Autentizační subsystém byl vestavěný do verze 2.50 systému REXYGEN. Uživatelé, role a pravomoce jsou definovány právě autentizačním subsystémem. Autentizační subsystém může být také připojený ke standardním účtům ze souborů `passwd/shadow` v prostředí GNU/Linux. Engine pro autentizační mechanismy PAM a LDAP je plánován, avšak zatím nepodporován. Konfigurační rozhraní uživatelských účtů je k dispozici v programech REXYGEN Studio a REXYGEN DWM.

5.1 Uživatelé a role

Jsou definovány následující pravomoce a role:

- *admin* - všechna oprávnění, uživatel s touto rolí může provést jakoukoli operaci a má plnou kontrolu nad cílovým zařízením.
- *super* - uživatel s touto rolí nemůže provádět operace, které mají dopad na cílové zařízení (tj. rebootovat zařízení, nastavit systémový čas atd.), ale stále může modifikovat běžící exekutivu,
- *operator* - uživatel s touto rolí nemůže modifikovat běžící exekutivu, ale může číst a měnit hodnoty signálů,
- *guest* - uživatel s touto rolí může pouze číst hodnoty signálů a nemůže provádět žádné změny.

Ve výchozím nastavení je aktivována pouze role *admin*. Pro aktivaci rolí *super*, *operator* a *guest* je nutno změnit příslušná nastavení `auth.super.enabled`, `auth.operator.enabled` a `auth.guest.enabled` na hodnotu 1. Pro každou roli je připraven uživatelský účet s korespondujícím jménem.

Ve výchozím nastavení je autentizační subsystém aktivován. Uživatel může systém deaktivovat nastavením `auth.enabled` na hodnotu 0. Výchozí heslo pro roli *admin* je prázdné a uživatel by si ho měl nastavit ihned po prvním přihlášení.

Uživatel musí poskytnout autentizační údaje (jméno a heslo) před připojením k cílovému zařízení z programů REXYGEN Studio, REXYGEN DWM a REXYGEN HMI Designer nebo před použitím vestavěného webového rozhraní. Při zadání nesprávných údajů systém vrátí chybu a připojení se přeruší.

5.2 Užití unixových účtů

V prostředí GNU/Linux může být autentizační subsystém připojený ke standardním účtům definovaných soubory `passwd/shadow` pomocí aktivování konfiguračního nastavení `auth.allowsystem`. Pro přidání uživatele ke specifické roli je nutno, aby byla přítomna odpovídající z následujících systémových skupin a uživatelský účet musí být součástí této skupiny:

- *admin* - `rex-admin`,
- *super* - `rex-super`,
- *operator* - `rex-operator`,
- *guest* - `rex-guest`.

V prostředí GNU/Linux může být kořenový systémový účet přiřazen v systému REXYGEN k účtu s rolí *admin* aktivováním konfiguračního nastavení `auth.allowroot`.

Příklad: Pro přiřazení systémového účtu "pi" zařízení Raspberry Pi k roli *admin* systému REXYGEN vytvořte systémovou skupinu "rex-admin" a přidejte uživatele "pi" jako člena pomocí příkazu "`usermod -a -G rex-admin pi`". Poté je možno se do systému REXYGEN přihlásit pomocí uživatelského jména "pi". Heslo lze změnit pomocí příkazu "`passwd`".

Kapitola 6

Zabezpečení

Protokol SSL by měl být využit vždy při komunikaci s cílovým zařízením prostřednictvím internetu nebo nedůvěryhodné sítě. Sám sebou podepsaný certifikát je vytvořen automaticky během instalačního procesu jak na GNU/Linux, tak na Windows zařízeních. Pokud je tento certifikát postačující, není nutno dělat nic dalšího.

Pokud je dostupný vlastní certifikát a privátní klíč, uživatel je musí umístit do konfiguračního adresáře **RexCore**. Soubor s certifikátem by měl být pojmenován **rexcore.cer** a soubor s privátním klíčem by měl být pojmenován **rexcore.key**. Oba dva by měly být ve formátu PEM. Služba **RexCore** by měla být restartována po každé změně certifikátu nebo privátního klíče.

Seznam obrázků

Literatura

- [1] REX Controls s.r.o.. *Funkční bloky systému REXYGEN – Referenční příručka*, 2020. [→](#).
- [2] REX Controls s.r.o.. *Začínáme s řídicím systémem REXYGEN*, 2020. [→](#).
- [3] REX Controls s.r.o.. *Začínáme se systémem REXYGEN na platformě Raspberry Pi*, 2020. [→](#).
- [4] REX Controls s.r.o.. *Začínáme se systémem REXYGEN na Debian*, 2020. [→](#).
- [5] REX Controls s.r.o.. *REXYGEN Studio – Uživatelská příručka*, 2020. [→](#).
- [6] REX Controls s.r.o.. *REST API systému REXYGEN – Referenční příručka*, 2020. [→](#).
- [7] REX Controls s.r.o.. *REXYGEN HMI – Uživatelská příručka*, 2020. [→](#).