




Seznam rizik/Risk list

	Hrozba / Threat	Řešení / Mitigation	Závaž- nost /Severity	Pravdě- podob- nost /Probability
1.	výpadek cloudových služeb, výpadek operátora Sigfox	<i>přechod na klasický mód, jako byl před nasazením systému na cílových zařízeních by mělo být rozpoznatelné, že spojení selhalo</i>	mírný dopad	malá pravděpodobnost
2.	jeden z dodavatelů velmi zadrazí nebo zpoplatní své služby	komponentový systém by měl mít schopnost nahrazení jednotlivých komponent jinými technologiemi. (např Sigfox Lorou, Google Firebase nahrazen Amazon web service apod) všechny tyto změny budou vyžadovat další vývoj.	mírný dopad	malá pravděpodobnost
3.	zcizení aplikace, zároveň se zcizením zařízení v garáži	nahrávání firmware do zařízení je jednosměrný proces. Získání firmware z odcizeného zařízení by bylo velice komplikované.	mírný dopad	malá pravděpodobnost
4.	selže systém rezervací	je potřeba mít možnost zobrazit, že systém rezervací nefunguje.	střední dopad	malá pravděpodobnost
5.	selže systém sledování parkovacích míst	je potřeba mít možnost určit, které čidlo nefunguje. Je potřeba, aby uživatelé měli možnost zjistit, že je hlášený problém, který se u čidla řeší. Toto čidlo by pak také mělo být nahraditelné jiným čidlem.	střední dopad	střední pravděpodobnost
6.	zařízení budou odcizena nebo poškozena	odcizená zařízení mohou být nahrazena novými zařízeními. po nahrání firmware, spárování a konfiguraci bude systém fungovat jako dříve. Ze systému bude zjistitelné, kdy došlo k poslední synchronizaci a kdy tedy došlo k poškození, nebo k odcizení.	mirný dopad	malá pravděpodobnost
7.	hackerský útok na systém	zaútočit je možné na více zařízení po cestě. 1. na BC DAQ node - vyžaduje překonání vstupní brány 2. na BC server node - vyžaduje překonání vstupní brány 3. na sigfox síť 4. na Google Firebase 5. na uživatelská zařízení Je málo pravděpodobné, že dojde k hackerkému útoku. Vyřazení systému by nemělo způsobit škody vlastníkov, a ani přínos útočníkovi. Nelze ale hackerský útok vyloučit. Z tohoto důvodu je na každém komponentu řešení implementováno alespoň základní zabezpečení. Zaútočení na 1 a 2 by muselo být spojené s překonáním vstupní brány a pozměněním zařízení, nebo jejich firmwaru. Zabezpečení proti zaútočení na bezdrátovou komunikaci mezi 1 a 2 je pomocí kryptočipu od BC Zaútočení na 3, 4 jsou zabezpečené pomocí SSL	mírný dopad	malá pravděpodobnost
8.				

9.				
10.				
11.				
12.				

Legenda/Legend

Závažnost /Severity

 malé low risk
  střední riziko/middle risk
  velké riziko/high risk

Pravděpodobnost / Probability

 malá pravděpodobnost/low
  střední pravděpodobnost /middle
  velká pravděpodobnost/high