

29 Dynamická analýza funkcí a parametrů pomocí nástroje ANaConDA

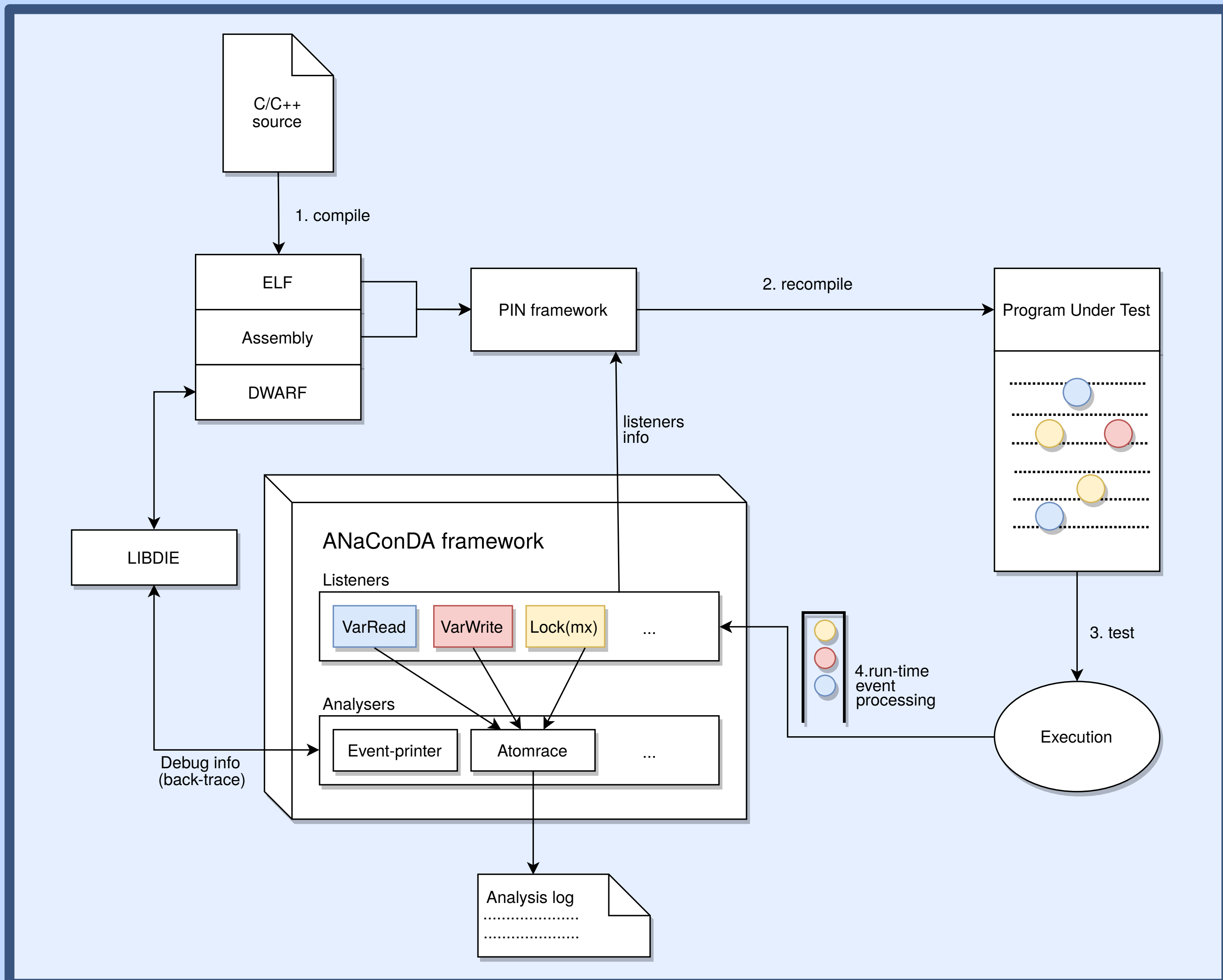
Framework ANaConDA

Adaptable Native-code
Concurrency-Focused
Dynamic Analysis

je prostředí poskytující podporu pro tvorbu dynamických analyzátorů a následnou dynamickou analýzu programů na binární úrovni napsaných v jazycích C/C++.

Umožňuje vytvářet analyzátoři pro testování vícevláknových programů a odhalování paralelních chyb.

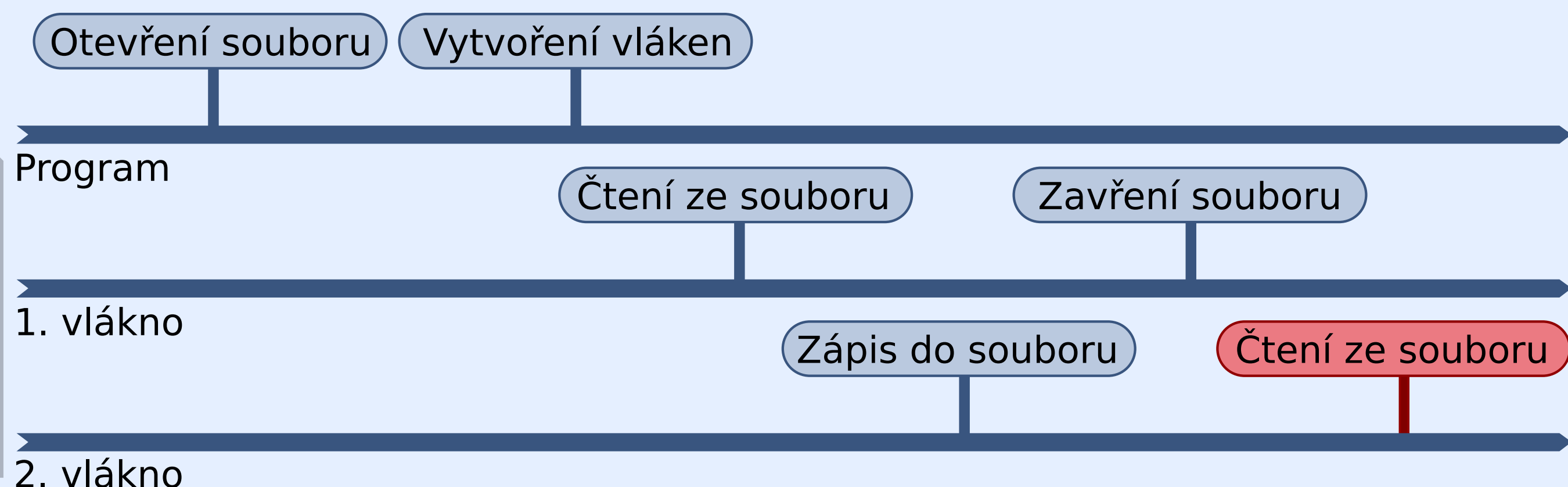
Poskytuje informace o běhu programu a událostech jako jsou přístupy do paměti nebo volání funkcí.



Příklad chyby nad soubory

```
FILE* fp; char buffer[255];

fp = fopen("fileName", "r+");
fprintf(fp, "Hello world!\n");
fgets(buffer, 255, fp);
fclose(fp);
```



Analýza funkcí a jejich parametrů

- Jedním ze zástupců paralelních chyb je nesprávné pořadí (order violation).
- Projevuje se při porušení pořadí operací, které je nutné pro korektní chování programu.
- Příklad znázorňuje chybu nad souborem, ale může se týkat libovolného objektu, datové struktury či kolekce.
- Pro detekci je nutné sledovat volání konkrétních funkcí včetně argumentů a návratových hodnot.