DIVINE: Průběžná zpráva

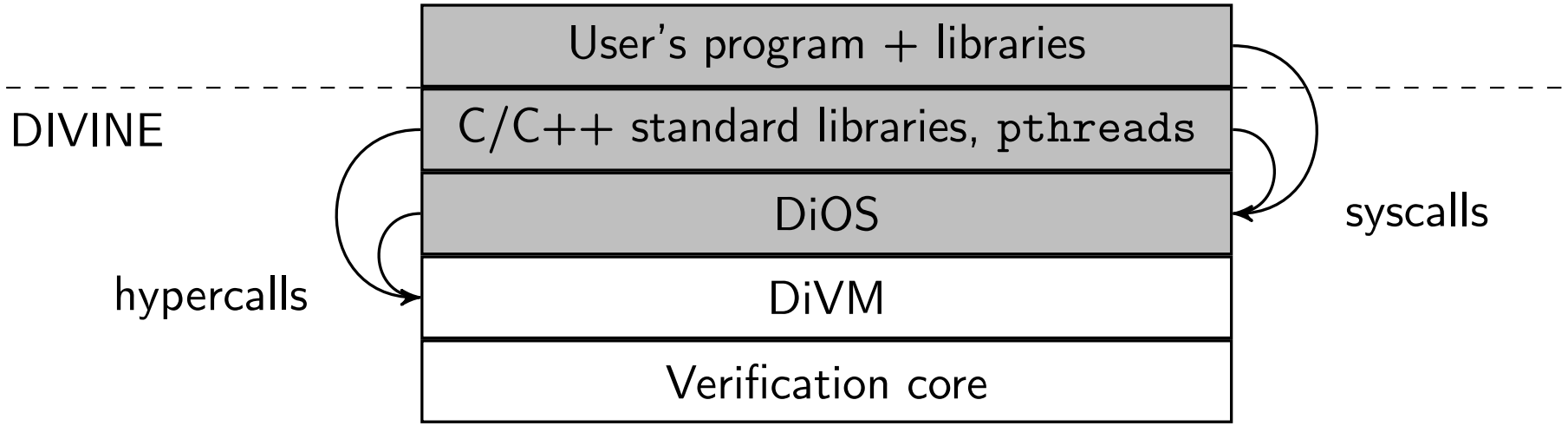
Vladimír Štill

Masarykova univerzita

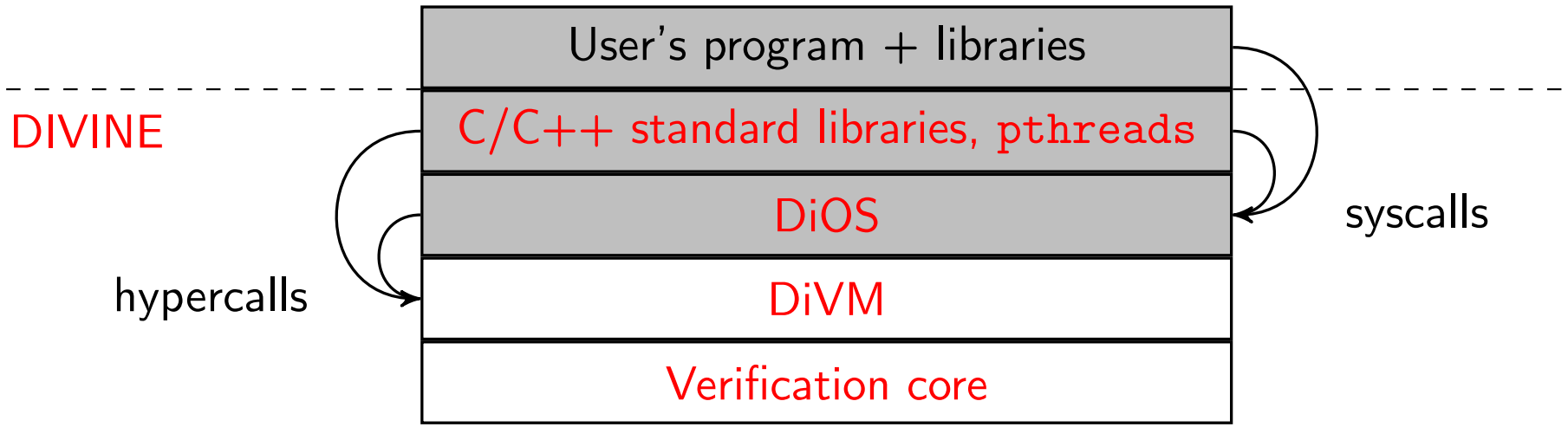
Brno, Česká republika

12. května 2017

Aktuální stav: implementace

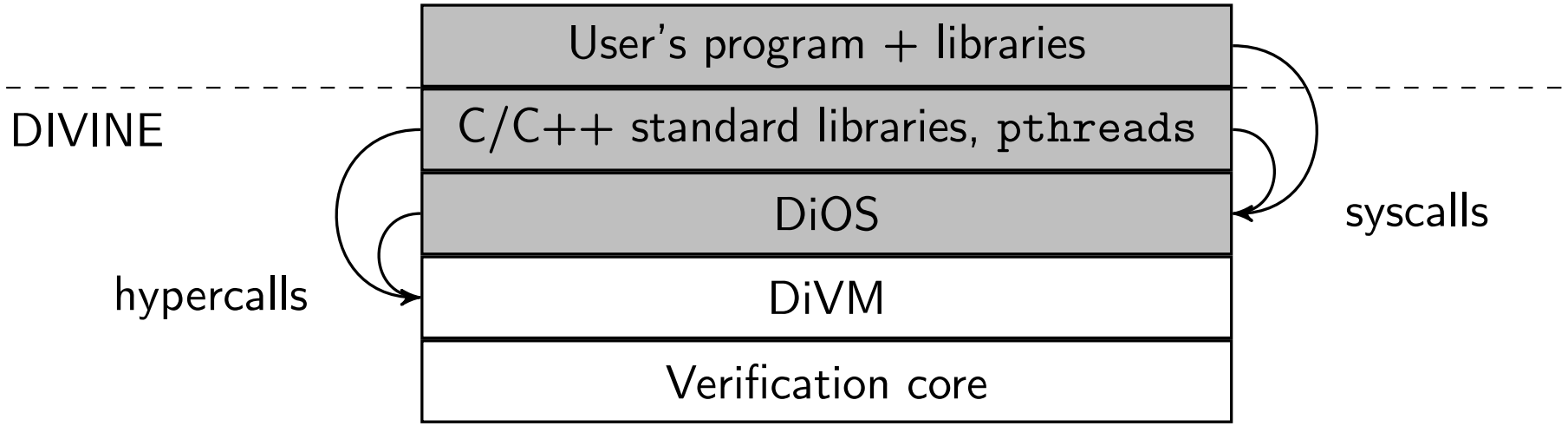


Aktuální stav: implementace



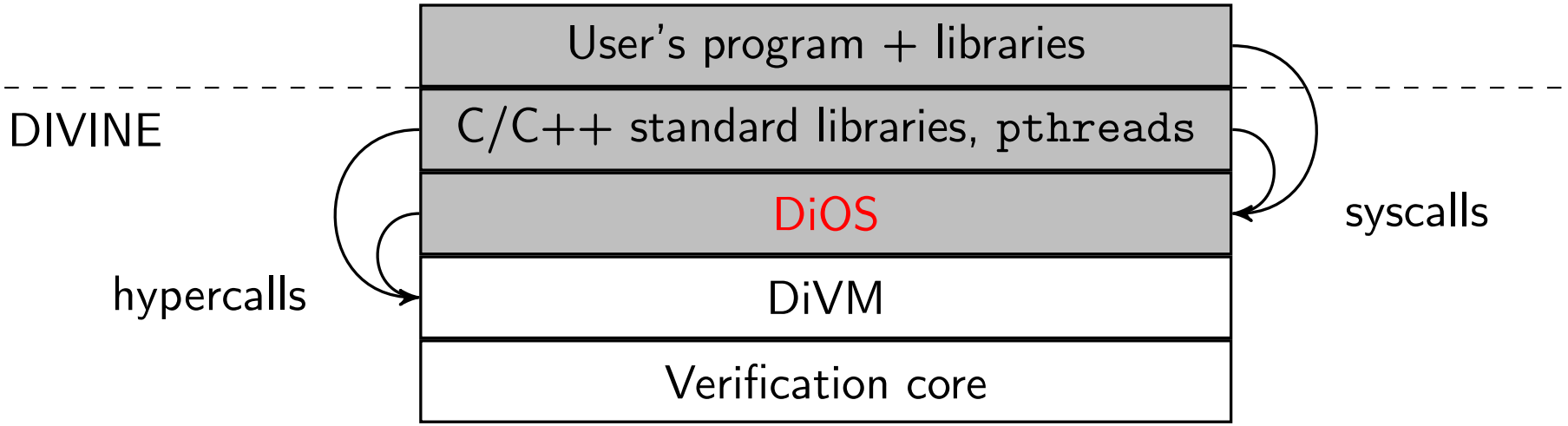
- DIVINE 4.0 final (9. 1.), aktuální je 4.0.7
- průběžná práce na podpoře symbolické verifikace (Henrich Lauko)
- modularizace DiOS (Jan Mrázek)
- záznam a přehrávání systémových volání (Katarína Kejstová)
- testy, benchmarky, evaluace (Vladimír Štill, Petr Ročkai, . . .)
- monitory, LTL (Tadeáš Kučera, Henrich Lauko)
- práce na procesech (Zuzana Baranová)

Aktuální stav: implementace



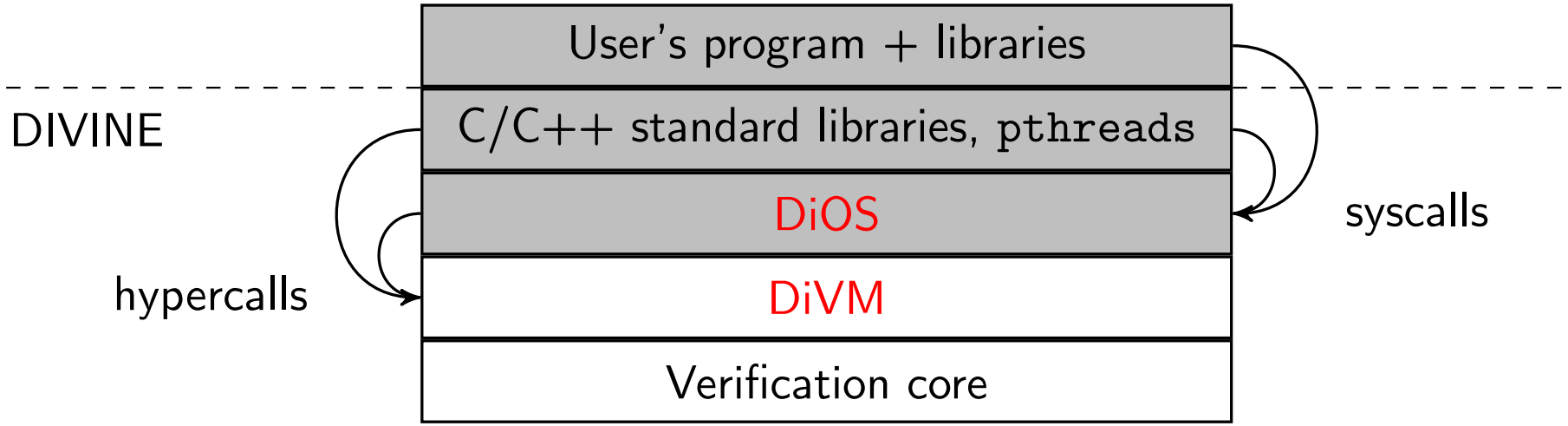
- DIVINE 4.0 final (9. 1.), aktuální je 4.0.7
- průběžná práce na podpoře symbolické verifikace (Henrich Lauko)
- modularizace DiOS (Jan Mrázek)
- záznam a přehrávání systémových volání (Katarína Kejstová)
- testy, benchmarky, evaluace (Vladimír Štill, Petr Ročkai, . . .)
- monitory, LTL (Tadeáš Kučera, Henrich Lauko)
- práce na procesech (Zuzana Baranová)

Aktuální stav: implementace



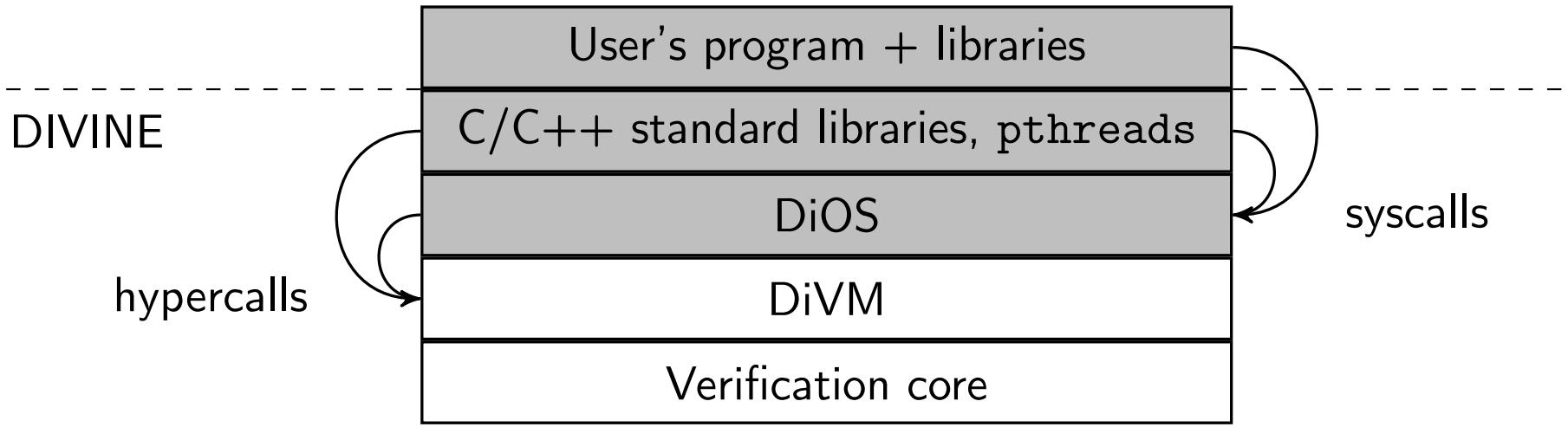
- DIVINE 4.0 final (9. 1.), aktuální je 4.0.7
- průběžná práce na podpoře symbolické verifikace (Henrich Lauko)
- modularizace DiOS (Jan Mrázek)
- záznam a přehrávání systémových volání (Katarína Kejstová)
- testy, benchmarky, evaluace (Vladimír Štill, Petr Ročkai, . . .)
- monitory, LTL (Tadeáš Kučera, Henrich Lauko)
- práce na procesech (Zuzana Baranová)

Aktuální stav: implementace



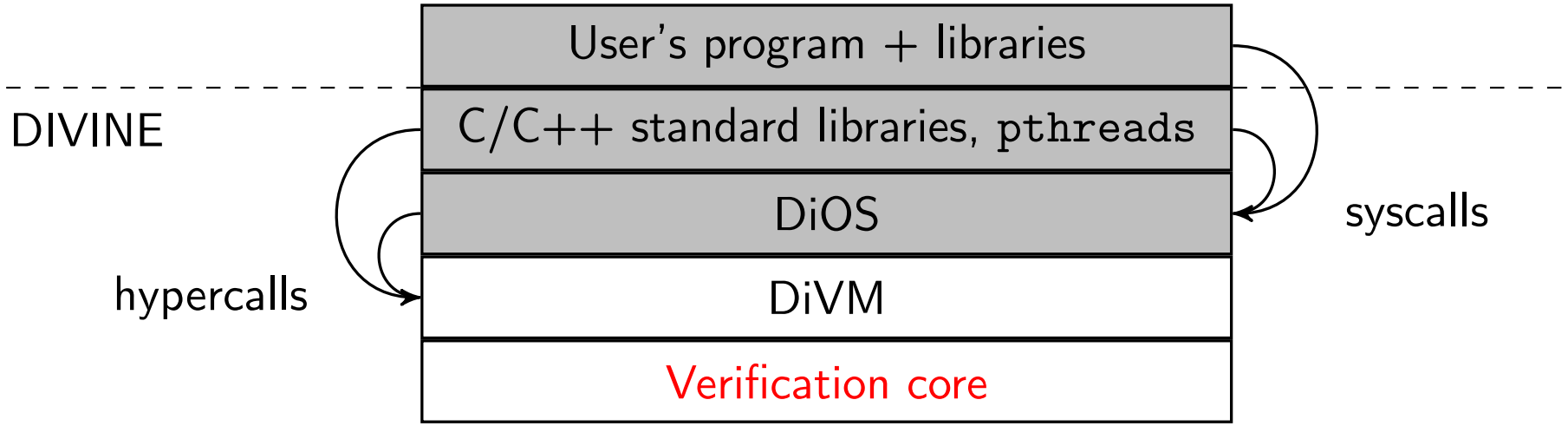
- DIVINE 4.0 final (9. 1.), aktuální je 4.0.7
- průběžná práce na podpoře symbolické verifikace (Henrich Lauko)
- modularizace DiOS (Jan Mrázek)
- záznam a přehrávání systémových volání (Katarína Kejstová)
- testy, benchmarky, evaluace (Vladimír Štill, Petr Ročkai, . . .)
- monitory, LTL (Tadeáš Kučera, Henrich Lauko)
- práce na procesech (Zuzana Baranová)

Aktuální stav: implementace



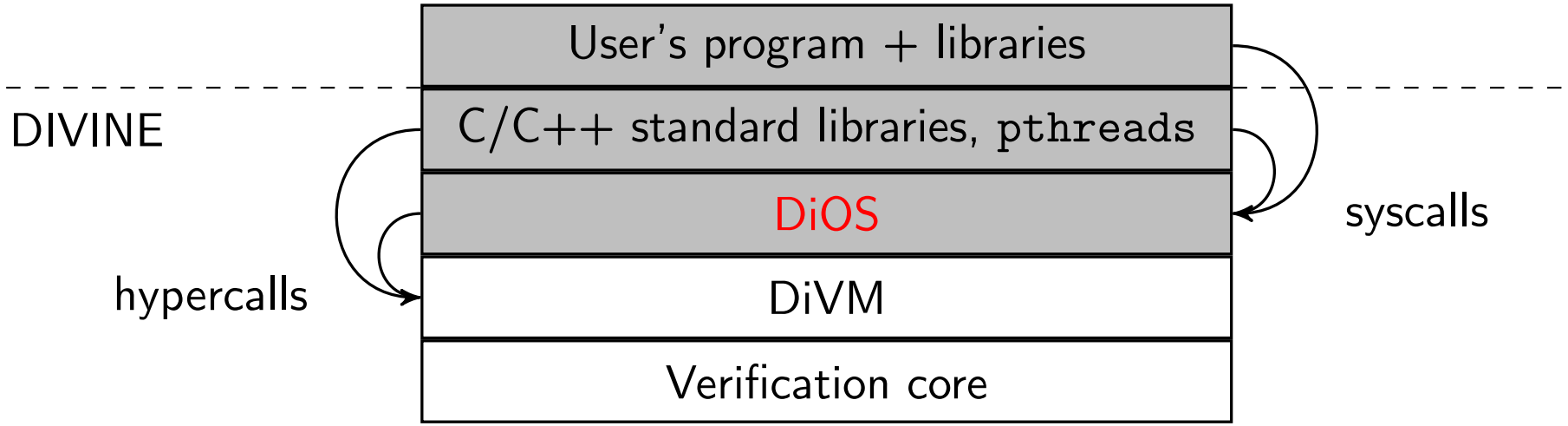
- DIVINE 4.0 final (9. 1.), aktuální je 4.0.7
- průběžná práce na podpoře symbolické verifikace (Henrich Lauko)
- modularizace DiOS (Jan Mrázek)
- záznam a přehrávání systémových volání (Katarína Kejstová)
- testy, benchmarky, evaluace (Vladimír Štill, Petr Ročkai, . . .)
- monitory, LTL (Tadeáš Kučera, Henrich Lauko)
- práce na procesech (Zuzana Baranová)

Aktuální stav: implementace



- DIVINE 4.0 final (9. 1.), aktuální je 4.0.7
- průběžná práce na podpoře symbolické verifikace (Henrich Lauko)
- modularizace DiOS (Jan Mrázek)
- záznam a přehrávání systémových volání (Katarína Kejstová)
- testy, benchmarky, evaluace (Vladimír Štill, Petr Ročkai, . . .)
- monitory, LTL (Tadeáš Kučera, Henrich Lauko)
- práce na procesech (Zuzana Baranová)

Aktuální stav: implementace



- DIVINE 4.0 final (9. 1.), aktuální je 4.0.7
- průběžná práce na podpoře symbolické verifikace (Henrich Lauko)
- modularizace DiOS (Jan Mrázek)
- záznam a přehrávání systémových volání (Katarína Kejstová)
- testy, benchmarky, evaluace (Vladimír Štill, Petr Ročkai, . . .)
- monitory, LTL (Tadeáš Kučera, Henrich Lauko)
- práce na procesech (Zuzana Baranová)

Aktuální stav: publikace

- Petr Ročkai, Vladimír Štill, Ivana Černá, Jiří Barnat:
  DiVM: Model Checking with LLVM and Graph Memory

Aktuální stav: publikace

- Petr Ročkai, Vladimír Štill, Ivana Černá, Jiří Barnat:
  DiVM: Model Checking with LLVM and Graph Memory

- Vladimír Štill, Petr Ročkai, Jiří Barnat:
  Using Off-the-Shelf Exception Support Components in C++ Verification

Aktuální stav: publikace

- Petr Ročkai, Vladimír Štill, Ivana Černá, Jiří Barnat:
  DiVM: Model Checking with LLVM and Graph Memory
- Vladimír Štill, Petr Ročkai, Jiří Barnat:
  Using Off-the-Shelf Exception Support Components in C++ Verification
- **Model Checking of C and C++ with DIVINE 4**

Aktuální stav: publikace

- Petr Ročkai, Vladimír Štill, Ivana Černá, Jiří Barnat:
  DiVM: Model Checking with LLVM and Graph Memory
- Vladimír Štill, Petr Ročkai, Jiří Barnat:
  Using Off-the-Shelf Exception Support Components in C++ Verification
- **Model Checking of C and C++ with DIVINE 4**
- Katarína Kejstová, Petr Ročkai, Jiří Barnat:
  From Model Checking to Runtime Verification and Back

Aktuální stav: publikace

- Petr Ročkai, Vladimír Štill, Ivana Černá, Jiří Barnat:
  DiVM: Model Checking with LLVM and Graph Memory
- Vladimír Štill, Petr Ročkai, Jiří Barnat:
  Using Off-the-Shelf Exception Support Components in C++ Verification
- **Model Checking of C and C++ with DIVINE 4**
- Katarína Kejstová, Petr Ročkai, Jiří Barnat:
  From Model Checking to Runtime Verification and Back
- Petr Ročkai, Jiří Barnat: **A Simulator for LLVM Bitcode**

(vše odesláno)

Aktuální stav: ostatní

účast na konferenci ETAPS/TACAS

- prezentace SymDIVINE na SV-COMP (Jan Mrázek)

Aktuální stav: ostatní

účast na konferenci ETAPS/TACAS

- prezentace SymDIVINE na SV-COMP (Jan Mrázek)

- novinky v SV-COMP
  - bez preprocessingu vstupních souborů
  - nově požadují svědky nekorektnosti ve všech kategoriích
    - zatím chybí validátory pro concurrency a memory safety
  - svědci korektnosti (ne všude)
  - LTL demo kategorie
  - DIVINE se pravděpodobně zúčastní

Aktuální stav: ostatní

účast na konferenci ETAPS/TACAS

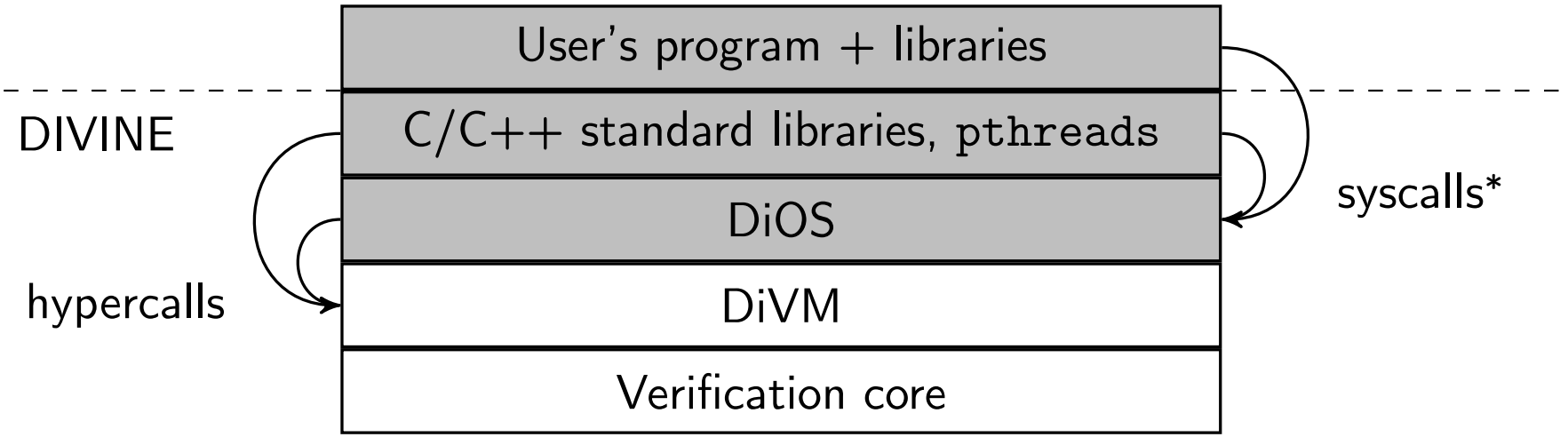
- prezentace SymDIVINE na SV-COMP (Jan Mrázek)

- novinky v SV-COMP
  - bez preprocessingu vstupních souborů
  - nově požadují svědky nekorektnosti ve všech kategoriích
    - zatím chybí validátory pro concurrency a memory safety
  - svědci korektnosti (ne všude)
  - LTL demo kategorie
  - DIVINE se pravděpodobně zúčastní

DIVINE v IA169 System Verification and Assurance

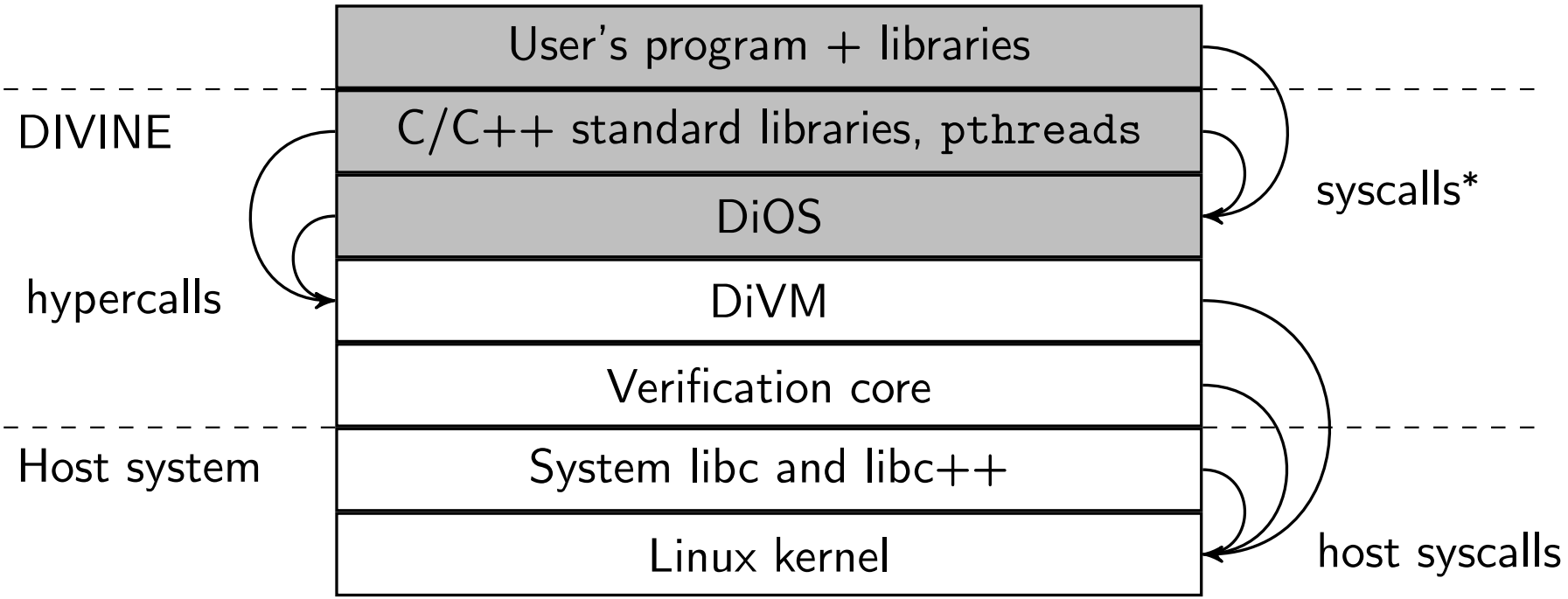
- cvičení o DIVINE s domácím úkolem
- feedback, především k simulátoru, odhalení drobných chyb
  - připomínky především k (ne)snadnosti debugování paralelních programů

Syscall Passthrough



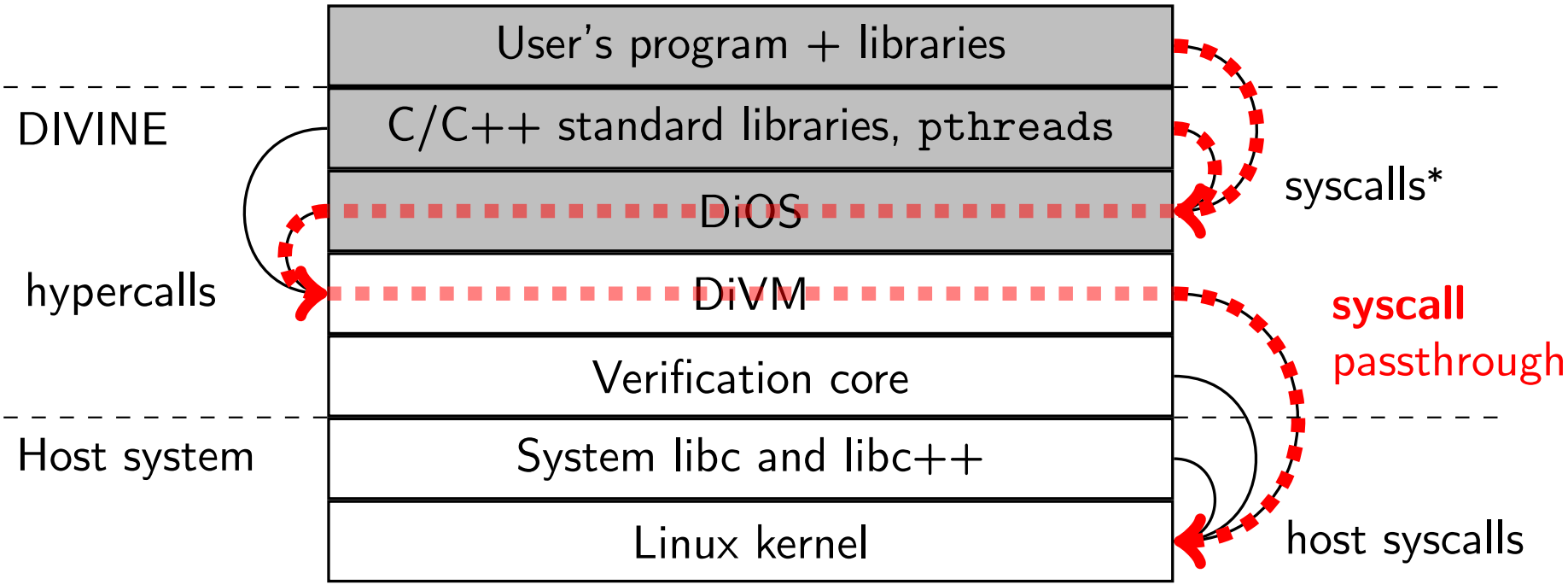
- (*): systémová volání DIVINE + simulovaná POSIX systémová volání

Syscall Passthrough



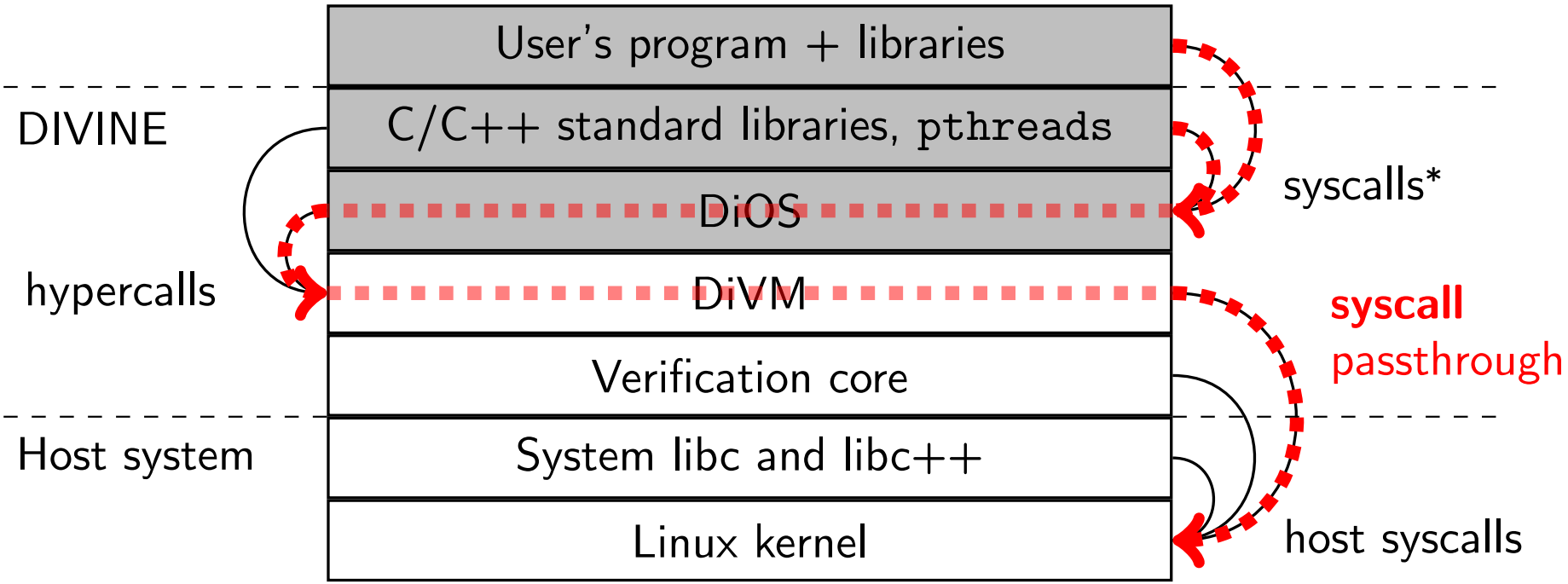
- (*): systémová volání DIVINE + simulovaná POSIX systémová volání

Syscall Passthrough



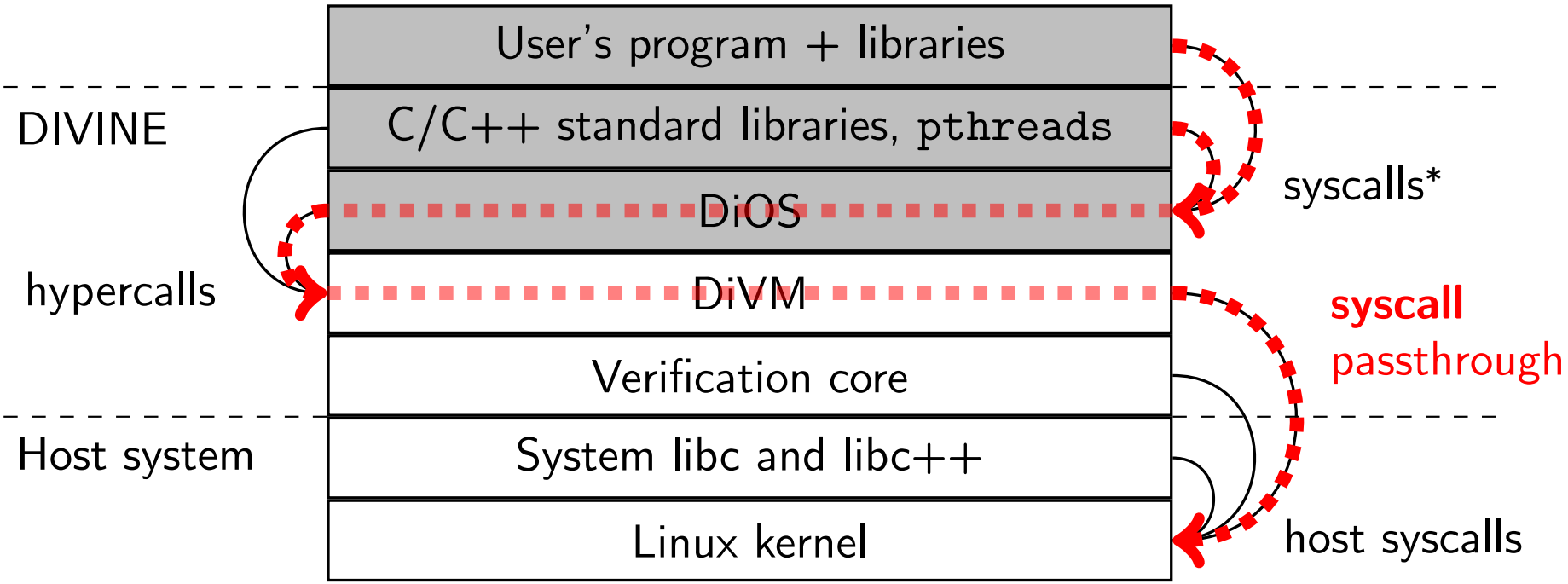
- (*): systémová volání DIVINE + provolávání POSIX systémových volání
- passthrough umožňuje volat skutečná systémová volání kernelu, na kterém DIVINE běží

Syscall Passthrough



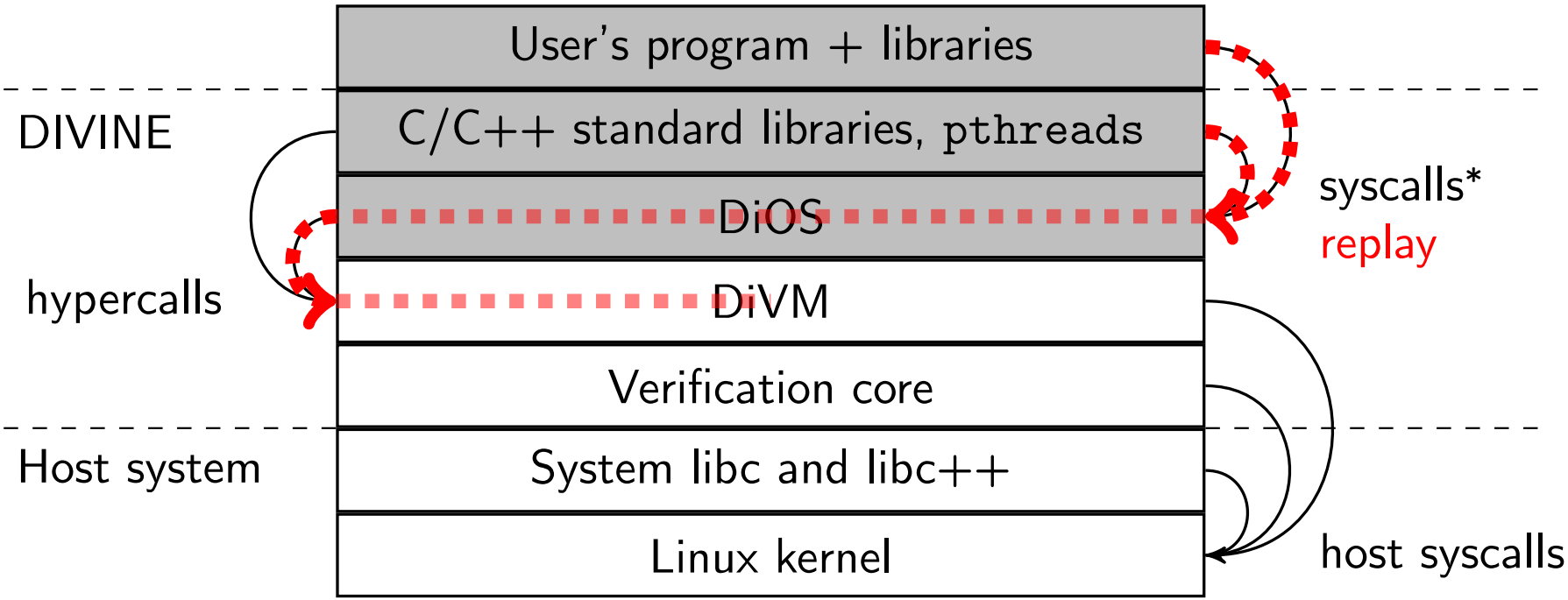
- (*): systémová volání DIVINE + provolávání POSIX systémových volání
- passthrough umožňuje volat skutečná systémová volání kernelu, na kterém DIVINE běží
  - v run módu DIVINE (jeden běh)

Syscall Passthrough



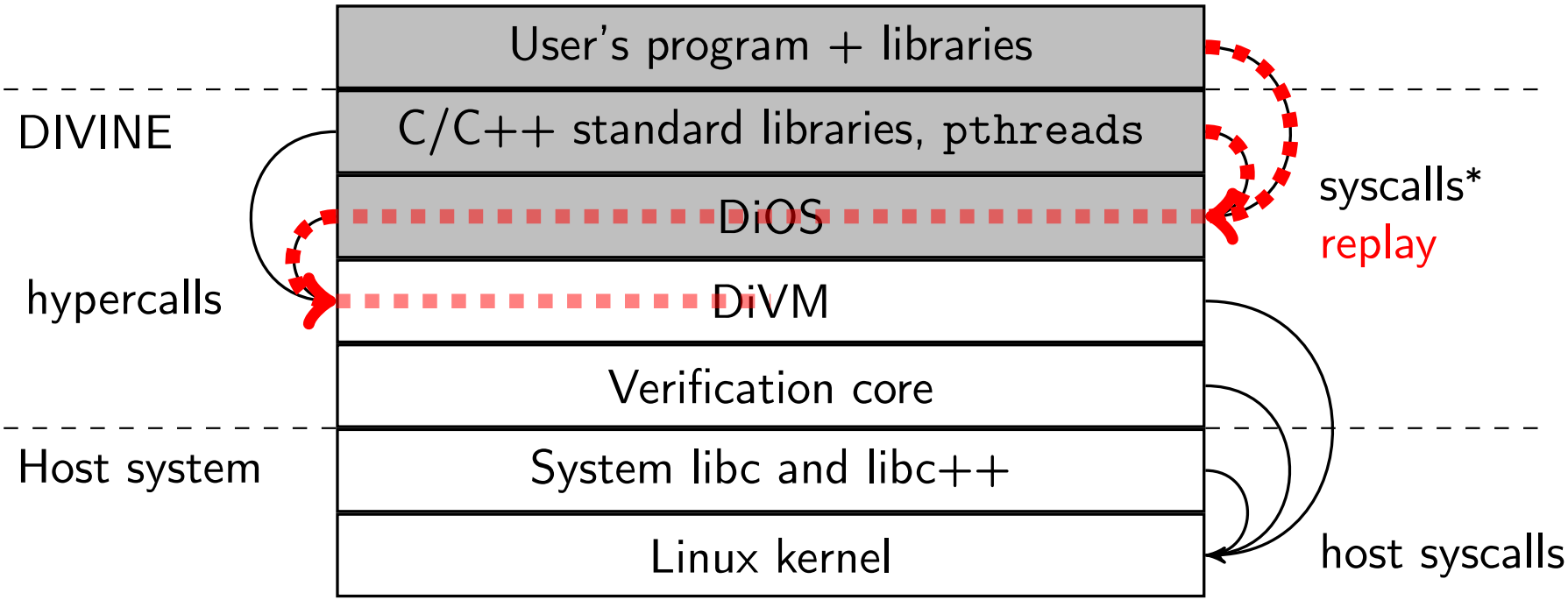
- (*): systémová volání DIVINE + provolávání POSIX systémových volání
- passthrough umožňuje volat skutečná systémová volání kernelu, na kterém DIVINE běží
  - v run módu DIVINE (jeden běh)
  - interakci se systémem lze nahrát

Syscall Passthrough



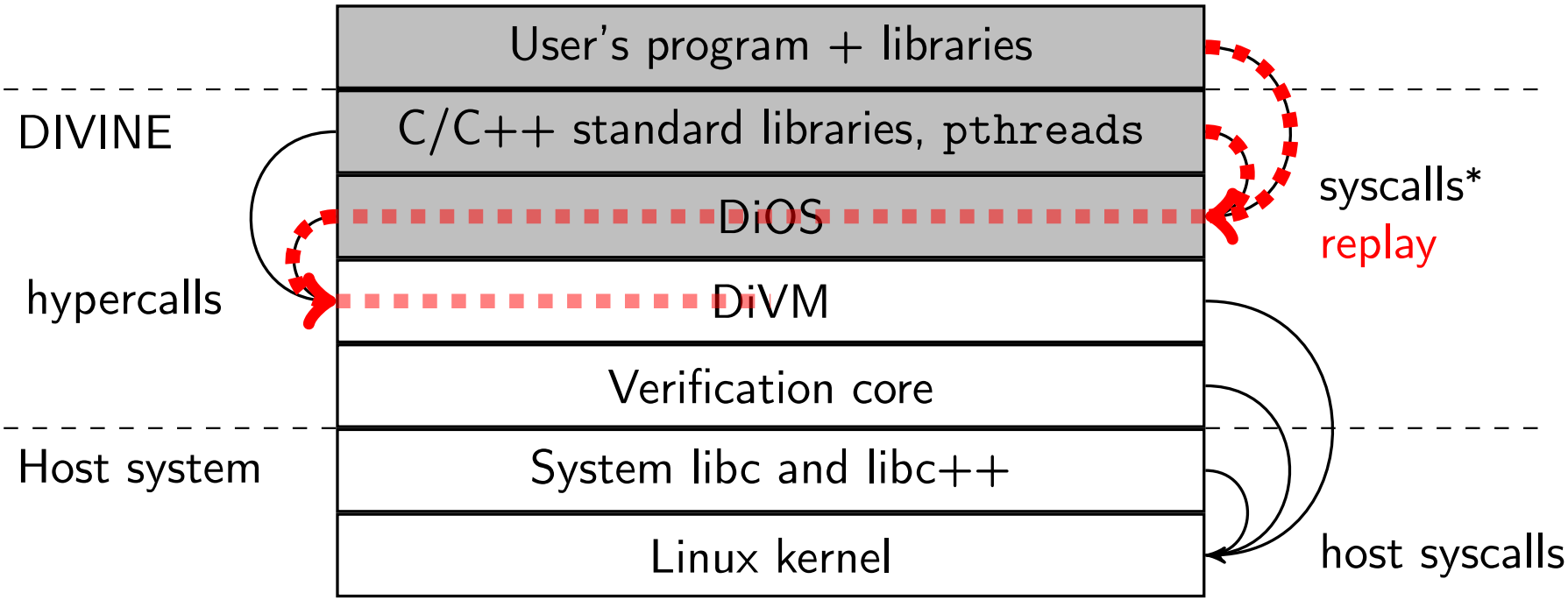
- (*): systémová volání DIVINE + přehrávání POSIX systémových volání
- passthrough umožňuje volat skutečná systémová volání kernelu, na kterém DIVINE běží
  - zaznamenanou interakci se systémem lze přehrát

Syscall Passthrough



- (*): systémová volání DIVINE + přehrávání POSIX systémových volání
- passthrough umožňuje volat skutečná systémová volání kernelu, na kterém DIVINE běží
  - zaznamenanou interakci se systémem lze přehrát
  - přehrávání funguje i ve `verify` a `sim`

Syscall Passthrough



- (*): systémová volání DIVINE + přehrávání POSIX systémových volání
- passthrough umožňuje volat skutečná systémová volání kernelu, na kterém DIVINE běží
  - zaznamenanou interakci se systémem lze přehrát
  - přehrávání funguje i ve `verify` a `sim`
  - může verifikovat běhy, které mají stejné (podobné) interakce

Plány

- verifikace se symbolickými daty, abstrakce
- vylepšování simulátoru, propojení s DiOS
- rozšiřování DiOS: procesy, konfigurovatelnost pro různé módy verifikace
- release-ready verze syscall passthrough
- verifikace LTL vlastností