Enclave模式的Rust-TEEOS

孙宇涛 安一帆 赖瀚宇

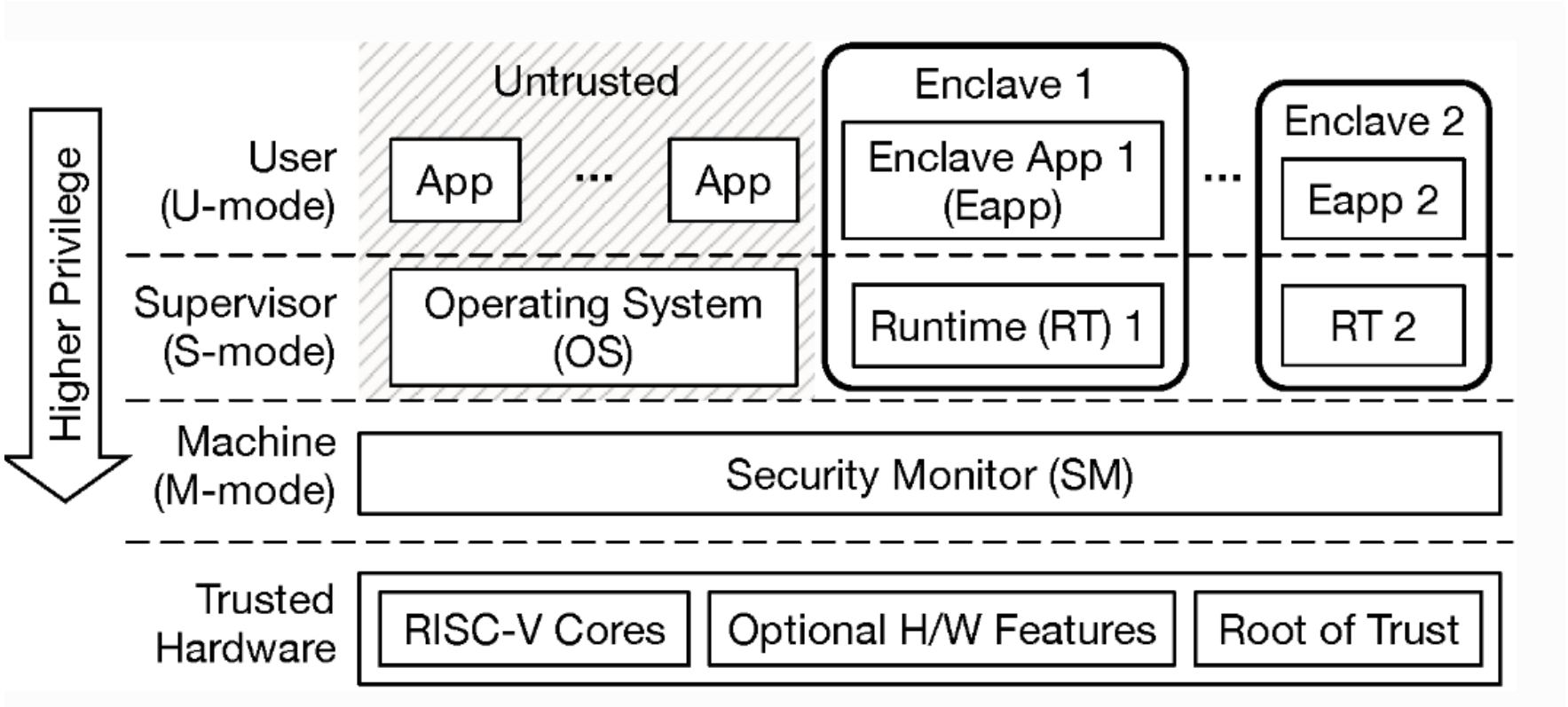
清華大學
Tsinghua University

CONTENTS

/01

系统运行逻辑

整体运行框架


Higher Privilege
User
(U-mode)
Supervisor
(S-mode)
Machine
(M-mode)
Trusted
Hardware
Untrusted
App
...
App
Operating System
(OS)
Enclave 1
Enclave App 1
(Eapp)
Runtime (RT) 1
...
Enclave 2
Eapp 2
RT 2
Security Monitor (SM)
RISC-V Cores
Optional H/W Features
Root of Trust

创建流程

- 创建Enclave
  - Host App计算Enclave所需的内存空间，Host OS在内存中开辟一块连续的内存提供给Enclave使用；
- 创建共享内存
  - 与私有内存相似；
- 确认创建完成
  - Host OS将若干参数传递给sbi层，分配和存储Enclave的必要信息，设置PMP内存隔离；
- 删除Enclave
  - 释放私有内存与共享内存，清除保存的相应数据结构，流程结束。

运行流程

- Host App发出运行信号，向下传递到sbi层，sbi层经过处理之后交给runtime运行；
- runtime收到时钟中断：
  - 暂停Enclave的运行，将控制权转交给sbi；
  - sbi再将控制权转交给Host OS，执行Host上的其他程序；
  - 时间片轮转到Host App时，恢复Enclave的运行；
- runtime收到Ocall（新增的系统调用，即Outbound Call）：
  - 将必要的信息复制到与Host App共享的内存中，发出sbi_call，将控制权转交给sbi；
  - sbi将控制权转交给Host OS；
  - Host OS将ocall信息传递给Host App，Host App （在SDK内部处理）根据预先设置好的方式处理后请求恢复Enclave的运行。

用户态交互

- 由于Runtime不是一个完整的操作系统，Enclave App与Host的交互是不可避免的；
- EApp依靠Edge Call在Host环境下执行相应的函数；
- EApp在共享内存中写入调用信息之后移交控制权给Host，Host检查共享内存之后执行调用；
- 调用方法为维护一个字典，其中保存了函数id与相应的函数地址，函数id在EApp开始执行时是已知的；

/02

Host OS的功能扩展

系统调用

- 在原有的Linux实现中，利用到了module的特性；
- 在基于zCore的实现中，类似地，将所有的操作封装为一个文件句柄，通过mmap和ioctl来进行实际的系统调用；
- 出于简单考虑，所有的Enclave系统调用均通过一个句柄，写死到系统中，fd=666；
- mmap的实现以及整个内存管理模式与zCore强耦合，相比于Linux上的实现做了较多修改；

内存管理

- 私有内存与共享内存需要分配连续的内存块，方便sbi和runtime进行处理；
- 最初的做法是，在初始化时，分配一个连续内存的vmo，在mmap时通过create_child进行虚拟地址的分配；
  - 但是，在zicron标准中对于contiguous的vmo进行create_child是禁止的！
  - 尝试修改这块代码使其变的可能，发现create_child嵌套的很深，修改很困难；
- 在初始化时，alloc若干个连续的物理页，在实际需要时（mmap时）再对其分配虚拟地址，修改页表；
  - 也配套修改了创建vmo的过程，但是这步是完全兼容的；
  - 在TEE需要的范围内，并不需要维护父子关系；

内核数据结构

- 内核需要管理一系列的Enclave的参数，以及id的分配：
  - 参考zCore的其他栈式分配系统，利用lazy_static创建一个全局管理器；
  - 由于需要频繁修改全局管理器所保存的参数，因此参考rCore的函数式编程来对其进行修改；
- 私有内存与共享内存的参数，相比于Linux上的实现做了较大修改：
  - 保存舒适化分配的若干PhysFrame组成的Vector，需要的时候对其进行切片；
  - 由于分配内存的时机不同，没有保存若干虚拟地址；

/03

SDK设计与实现

SDK结构设计

- SDK根据调用环境分为Host SDK和Enclave SDK；
- 根据前述系统设计，Host App通过调用SDK创建Enclave环境，Enclave App通过SDK实现Ocall。

SDK实现

- 具体实现上SDK分为三部分：
  - Host部分实现了创建Enclave所需的准备，包括：
    - 向Host OS请求分配内存；
    - 创建Enclave环境的页表；
    - 加载runtime和Enclave App的数据；
    - 注册负责处理Ocall的函数；
    - 实现启动和管理Enclave App的逻辑、处理Ocall等；
  - Enclave部分提供了调用Ocall的接口和结束Enclave App的接口；
  - Edge部分实现了Ocall的底层结构。

/04

Sbi的独立开发

SM API

- 包含 8 个接口:
- sbi_sm_create_enclave
- sbi_sm_destroy_enclave
- sbi_sm_run_enclave
- sbi_sm_exit_enclave
- sbi_sm_stop_enclave
- sbi_sm_resume_enclave
- sbi_sm_attest_enclave
- sbi_sm_get_sealing_key

platform

- generic (qemu)：较简单，不需特殊的硬件实现
- platform_create_enclave
- platform_destroy_enclave
- platform_init_enclave
- platform_switch_from_enclave
- platform_switch_to_enclave

enclave

- copy_enclave_create_args
- create_enclave
- destroy_enclave
- run_enclave
- exit_enclave
- resume_enclave
- attest_enclave
- copy_enclave_data
- context_switch_to_enclave
- context_switch_to_host

PMP（Physical memory protection）

- PMP_SET
- PMP_UNSET
- PMP_ERROR
- detect_region_overlap
- bitmap操作（set, unset, test)

```
struct pmp_region {
    size: u64,
    addrmode: u8,
    addr: u32,
    allow_overlap: i32,
    reg_idx: i32
}
```

MPRV（Modify PRiVilege）

- fn copy_block_from_sm(a: usize, b: *const mprv_block) -> i32;
- fn copy_word_from_sm(a: usize, b: *const usize) -> i32;
- fn copy1_from_sm(a: usize, b: *const u8) -> i32;

- fn copy_block_to_sm(dst: *const mprv_block, src: usize) -> i32;
- fn copy_word_to_sm(dst: *const usize, src: usize) -> i32;
- fn copy1_to_sm(dst: *const u8, src: usize) -> i32;

opensbi

- 手动实现使用到 opensbi 的接口（rustsbi未实现）：
- riscv_fence
- csr_read / csr_write
- csr_clear / csr_set
- spin_lock / spin_unlock
- current_hartid
- sbi_hart_hang
- sbi_memset / sbi_memcpy
- sbi_platform_hart_count

难点

- ipi（Inter-Processor Interrupt）
- 硬件相关代码（ex: sbi_platform_hart_count）
- 汇编代码：_trap_handler、trap_vector_enclave

总结

- 由于缺乏系统级的开发经验，在环境配置、编译选项等环节踩了不少坑；
- TEE的实现与运行流程较为复杂，调试困难，因此后期进程缓慢，没有完成后续的目标；
- 整体上更加偏向工程，对于其他TEE的实现缺乏了解，论文阅读效率很低；
- 可以看出Keystone在实现与设计上的一些缺陷，如果未来有机会继续这项工作，可能的规划为：
  - 将runtime自己实现一遍；
  - 改进Host OS和Host App的交互机制；
  - 改进用户态交互的机制，增强or修改runtime的能力；
  - ……
- 感谢陈渝、向勇老师的指导与建议，感谢贾越凯、王润基助教的答疑！

Click to edit Master title style

Text here

Unified fonts make reading more fluent.
Theme color makes PPT more convenient to change.
Adjust the spacing to adapt to Chinese typesetting, use the reference line in PPT.

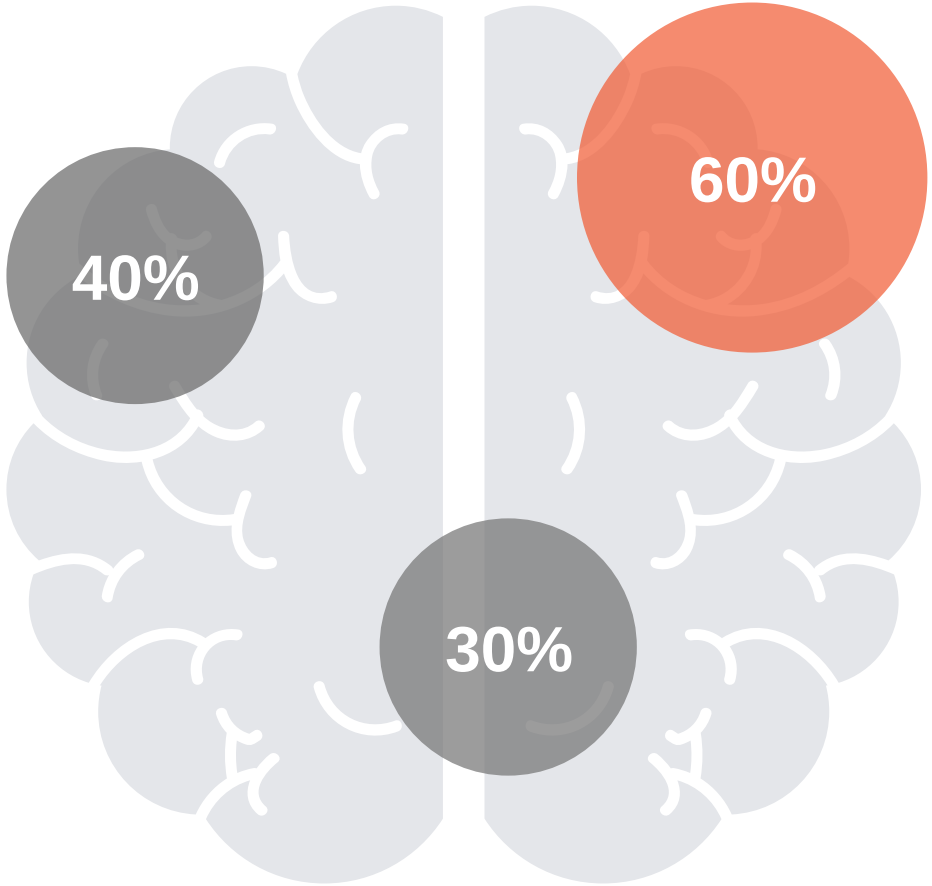
Click to edit Master title style

Text here

Unified fonts make reading more fluent.

Theme color makes PPT more convenient to change.

Adjust the spacing to adapt to Chinese typesetting, use the reference line in PPT.



Text here

- Supporting text here.
- ……

Text here

- Supporting text here.
- ……

Text here

- Supporting text here.
- ……

Click to edit Master title style

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Click to edit Master title style

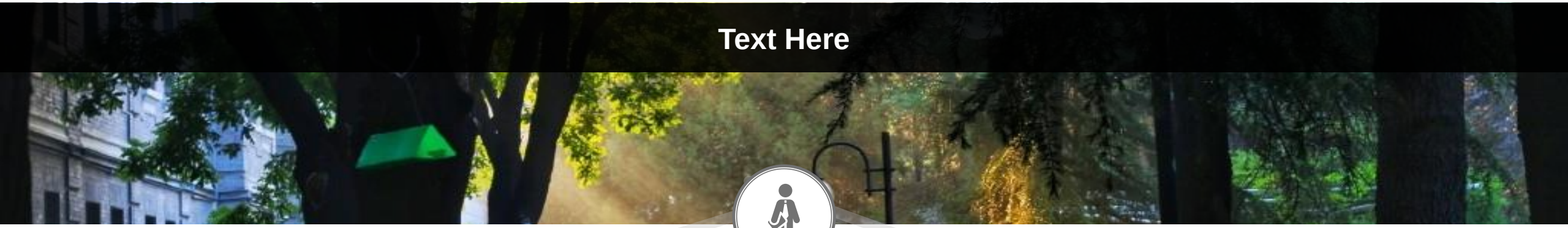
Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.
- ……

Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.
- ……

Click to edit Master title style



Text Here

Copy paste fonts. Choose the only option to retain text.

Text Here

Copy paste fonts. Choose the only option to retain text.

Text Here

Copy paste fonts. Choose the only option to retain text.

Text Here

Copy paste fonts. Choose the only option to retain text.

Click to edit Master title style

01.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

02.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

03.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

04.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Click to edit Master title style

Tsinghua University

Text here

Copy paste fonts. Choose the only option to retain text.

……

Text here

Copy paste fonts. Choose the only option to retain text.

……

2015

2016

2017

2018

Text here

Copy paste fonts. Choose the only option to retain text.

……

Text here

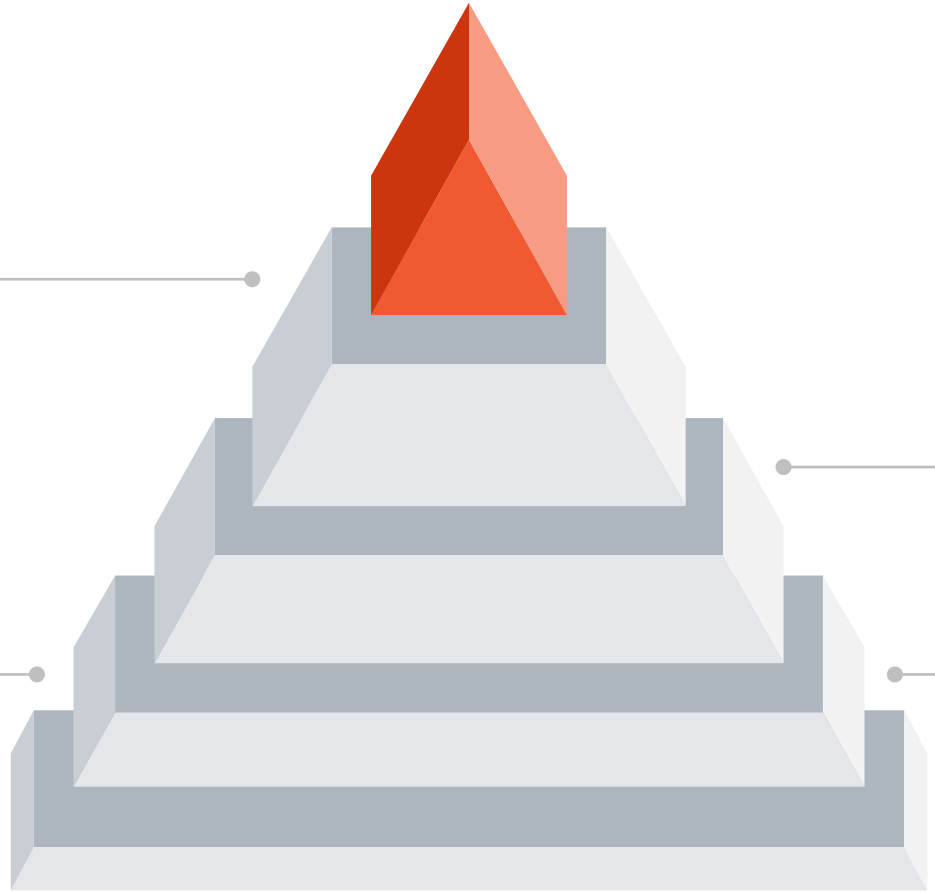
Copy paste fonts. Choose the only option to retain text.

……

Click to edit Master title style

Tsinghua University

$8,200



2018 Q1

Copy paste fonts. Choose the only option to retain text.

……

2018 Q2

Copy paste fonts. Choose the only option to retain text.

……

2018 Q3

Copy paste fonts. Choose the only option to retain text.

……

2018 Q4

Copy paste fonts. Choose the only option to retain text.

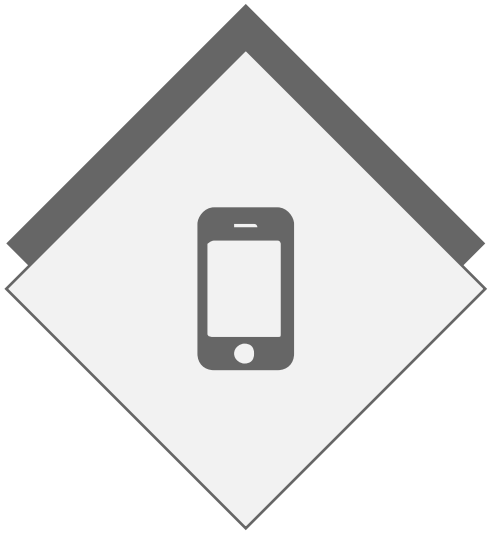
……

Click to edit Master title style

清華大學
Tsinghua University

Text here

Copy paste fonts. Choose the only option to retain text.

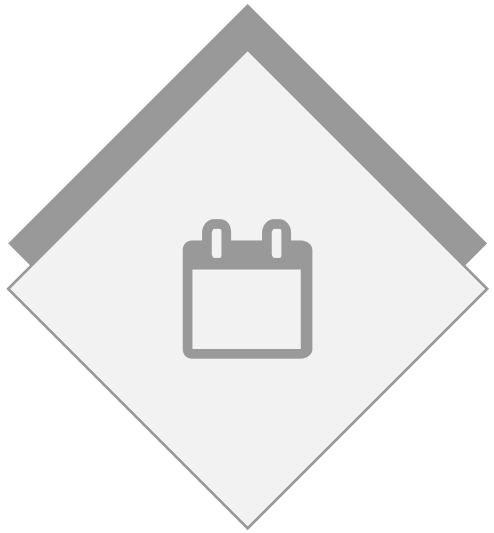


Text here

Copy paste fonts. Choose the only option to retain text.

Text here

Copy paste fonts. Choose the only option to retain text.



Text here

Copy paste fonts. Choose the only option to retain text.

/03

Section Header Here

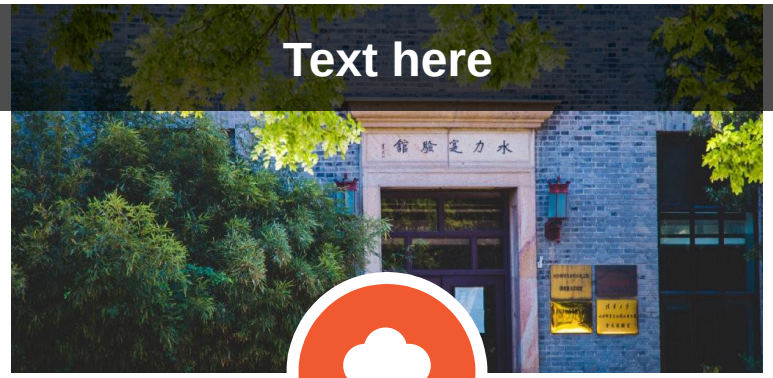
Supporting text here.

When you copy & paste, choose "keep text only" option.

Click to edit Master title style

Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.



Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.

Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.

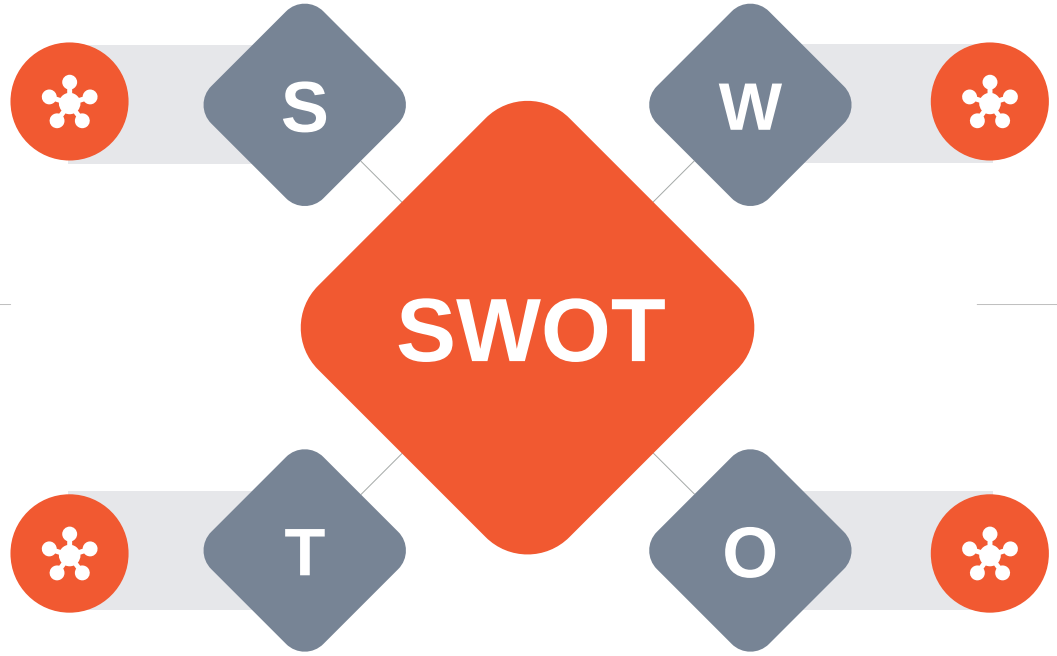
Click to edit Master title style

Text here

- Supporting text here.
- ……

Text here

- Supporting text here.
- ……



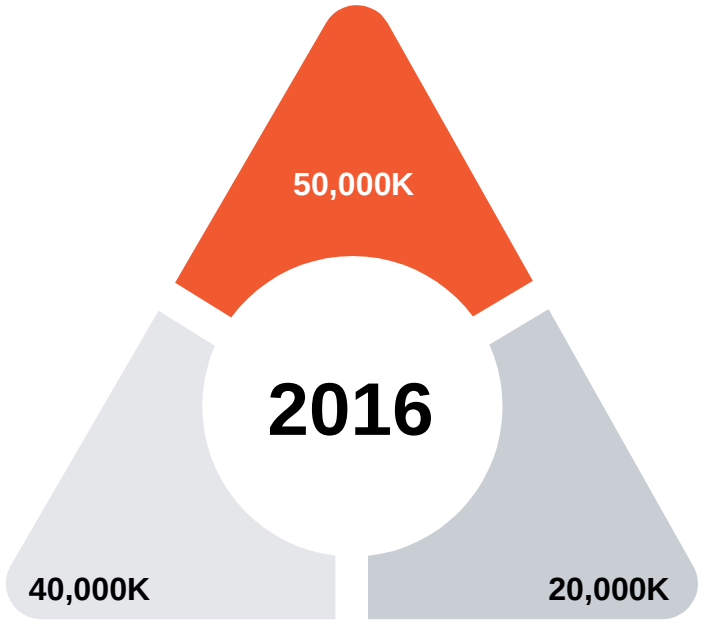
Text here

- Supporting text here.
- ……

Text here

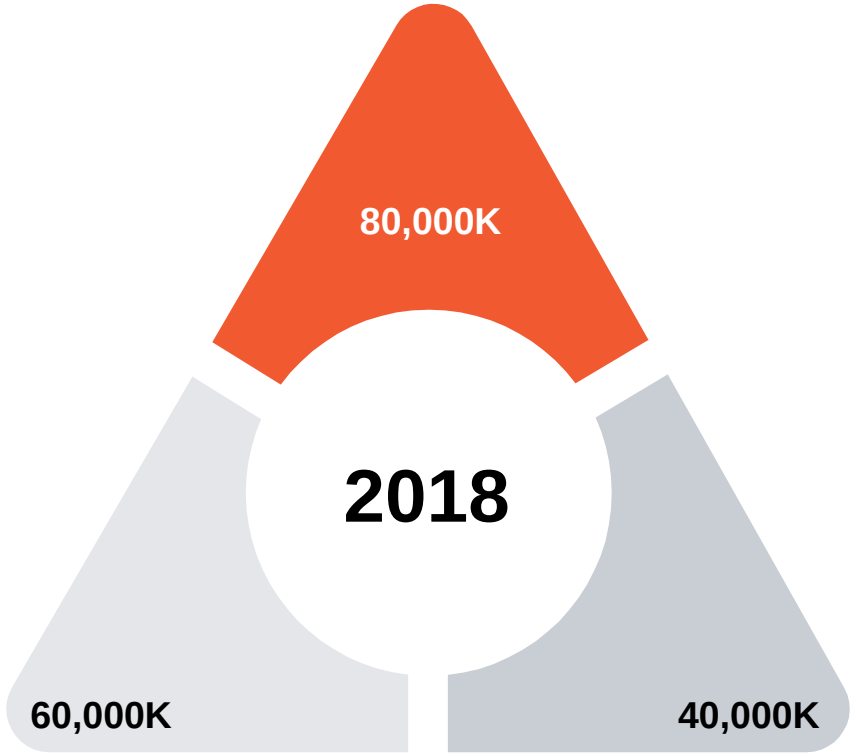
- Supporting text here.
- ……

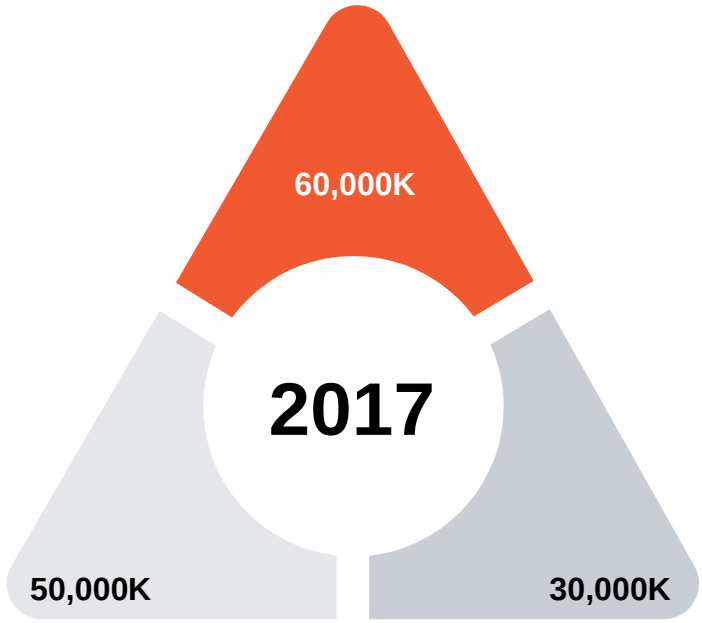
Click to edit Master title style



Text here

- Copy paste fonts. Choose the only option to retain text.
- ……



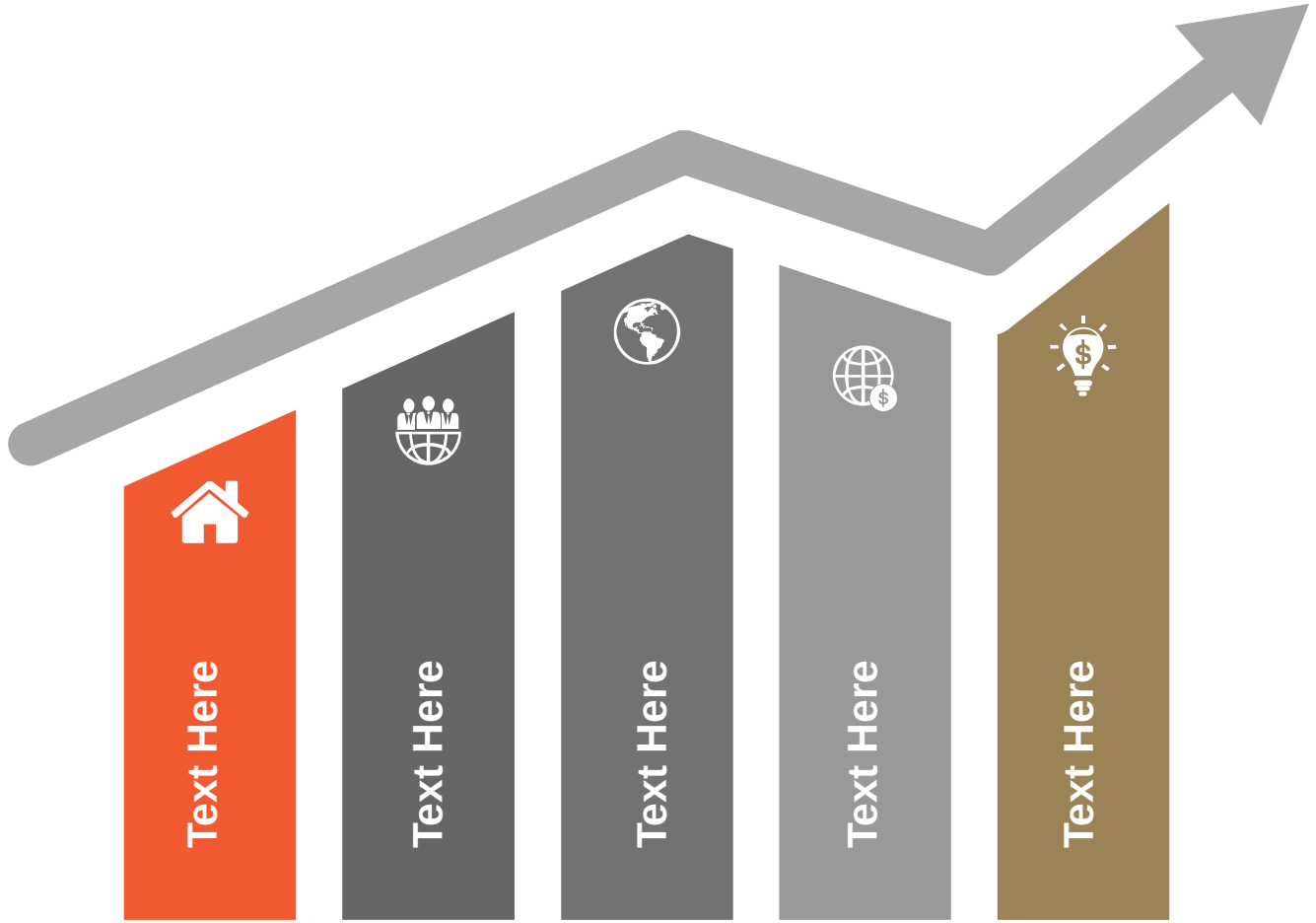


Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here Text here Text here

Click to edit Master title style



Text Here

Copy paste fonts. Choose the only option to retain text.

Text Here

Copy paste fonts. Choose the only option to retain text.

Text Here

Copy paste fonts. Choose the only option to retain text.

Text Here

Copy paste fonts. Choose the only option to retain text.

Text Here

Copy paste fonts. Choose the only option to retain text.

Click to edit Master title style

Tsinghua University

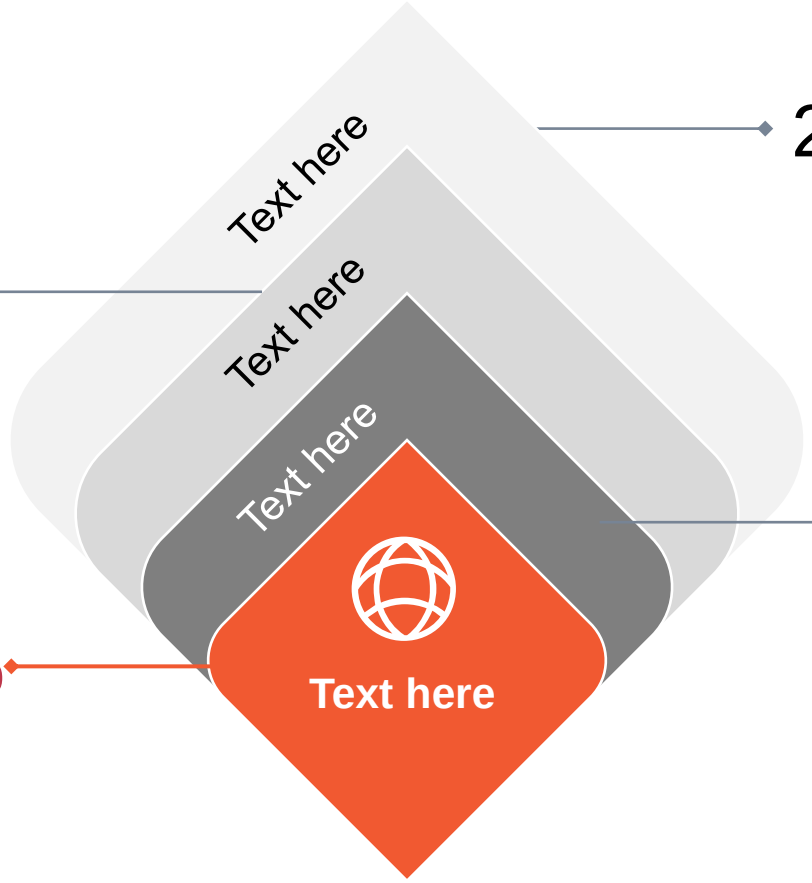
Text here

Copy paste fonts. Choose the only option to retain text.....

25%

Text here

Copy paste fonts. Choose the only option to retain text.....



25%

Text here

Copy paste fonts. Choose the only option to retain text.....

25%

Text here

Copy paste fonts. Choose the only option to retain text.....

/04

Section Header Here

Supporting text here.

When you copy & paste, choose "keep text only" option.

Click to edit Master title style

Text here

Unified fonts make reading more fluent.

Theme color makes PPT more convenient to change.

Adjust the spacing to adapt to Chinese typesetting, use the reference line in PPT.

Text Here

Supporting text here.

When you copy & paste, choose "keep text only" option.

Text Here

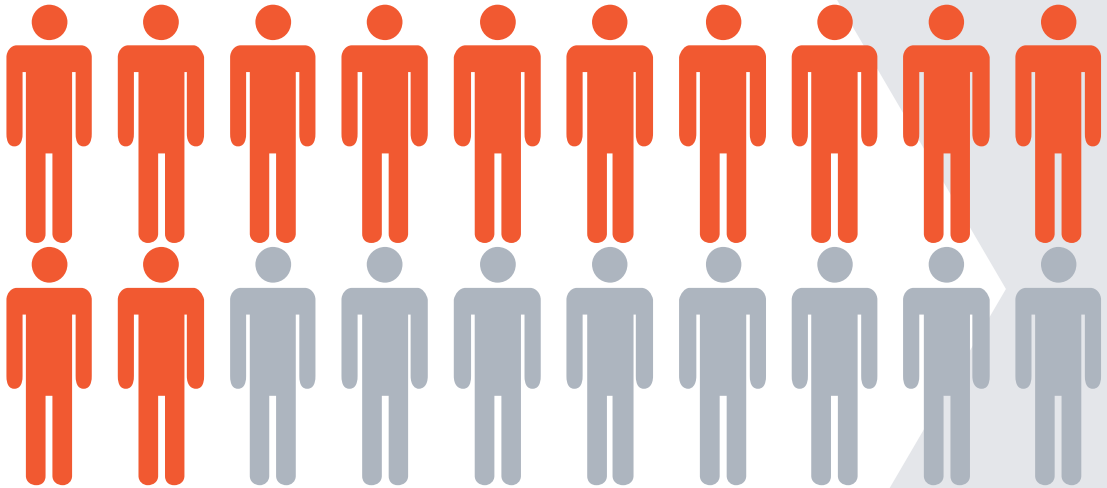
Supporting text here.

When you copy & paste, choose "keep text only" option.

Click to edit Master title style

60%

Text here



Text here

Unified fonts make reading more fluent.

Theme color makes PPT more convenient to change.

Adjust the spacing to adapt to Chinese typesetting, use the reference line in PPT.

01.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

02.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Click to edit Master title style

Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.

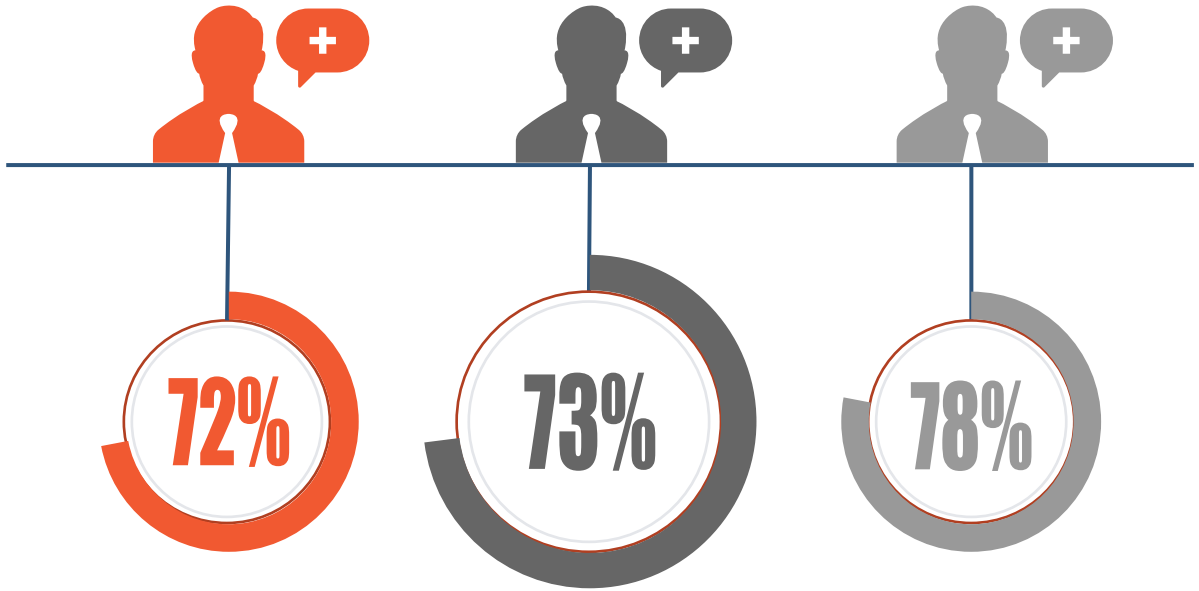
Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.

Text here

- Supporting text here.
- When you copy & paste, choose "keep text only" option.

Click to edit Master title style



TEXT HERE

Supporting text here

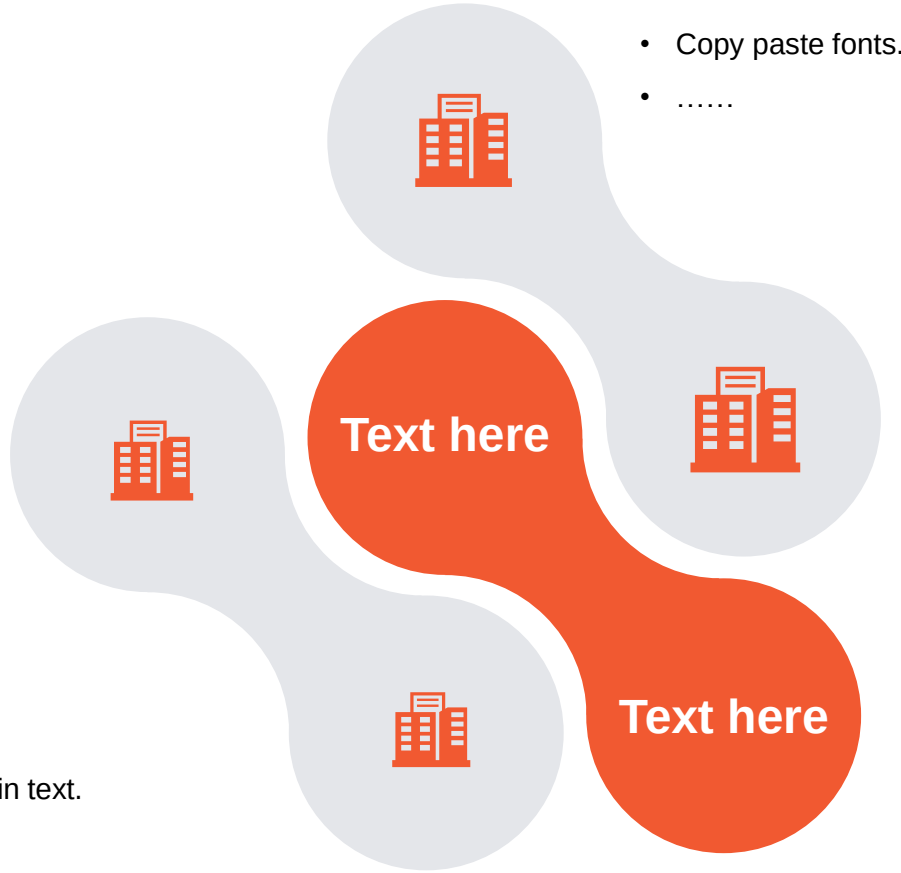
Click to edit Master title style

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……



Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

/05

Section Header Here

Supporting text here.

When you copy & paste, choose "keep text only" option.

Click to edit Master title style

Text here

Text	Text	Text
Text	Text	Text

Text here

Text	Text	Text

Text here

Text	Text	Text
Text	Text	Text

Click to edit Master title style

Text here

Unified fonts make reading more fluent.

Theme color makes PPT more convenient to change.

Adjust the spacing to adapt to Chinese typesetting, use the reference line in PPT.

01.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

02.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

03.Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Click to edit Master title style

60%

Text here

Copy paste fonts. Choose the only option to retain text.

……

40%

Text here

Copy paste fonts. Choose the only option to retain text.

……

20%

Text here

Copy paste fonts. Choose the only option to retain text.

……

Click to edit Master title style

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

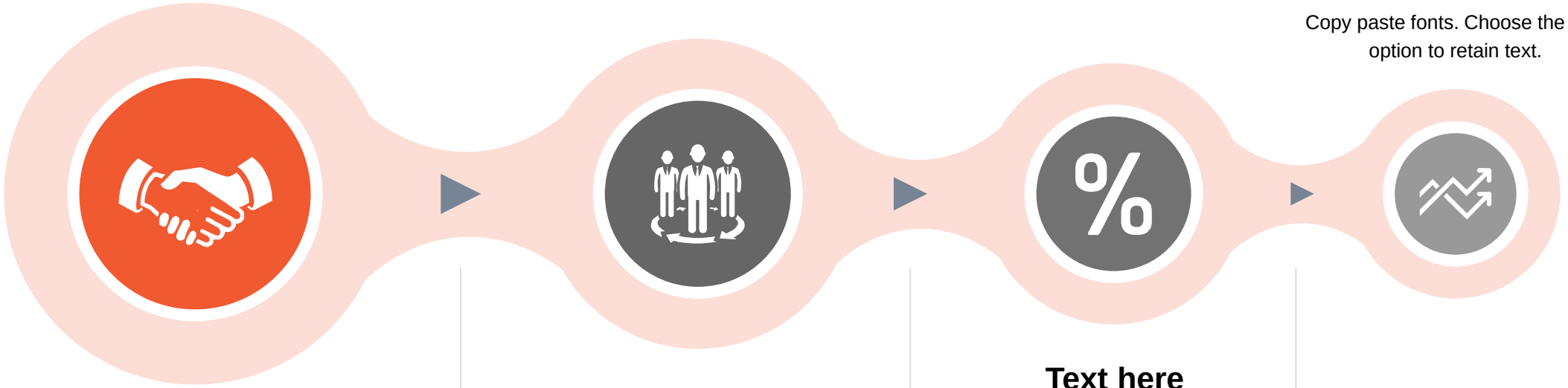
Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Text here

- Copy paste fonts. Choose the only option to retain text.
- ……

Click to edit Master title style



Text here

Copy paste fonts. Choose the only option to retain text.

Text here

Copy paste fonts. Choose the only option to retain text.

Text here

Copy paste fonts. Choose the only option to retain text.

Text here

Copy paste fonts. Choose the only option to retain text.