【软件构造】第七章第一节 健壮性和正确性的区别

第七章第一节 健壮性和正确性的区别

第七章：进入软件构造最关键的质量特性 ——健壮性和正确性。

本节在1-2节的基础上，重申了Robustness and Correctness的重要性，澄清了二者之 间的差异，并指明了在软件构造中处理二 者的典型技术（防御式编程、异常处理、 测试、调试等）

Outline

- 健壮性(Robustness)和正确性(correctness)
- 如何测量健壮性和正确性

Notes

健壮性(Robustness)和正确性(correctness)

【健壮性】

- 定义：系统在不 正常输入或不正常外部环境下仍能够表现正常的程度
- 面向健壮性编程：
  - 处理未期望的行为和错误终止
  - 即使终止执行，也要准确/无歧义的向用户展示全面的错误信息
  - 错误信息有助于进行debug
- 健壮性原则：
  - Paranoia (偏执狂)：总是假定用户恶意、假定自己的代码可能失败
  - 把用户想象成白痴，可能输入任何东西（返回给用户的错误提示信息要详细、准确、无歧义）
  - 对别人宽容点，对自己狠一点（对自己的代码要保守，对用户的行为要开放）
- 面向健壮性编程的原则：
  - 封闭实现细节，限定用户的恶意行为
  - 考虑极端情况，没有“不可能”

【正确性】

- 含义：程序按照spec加以执行的能力，是最重要的质量指标！
- 对比健壮性和正确性：
  - 正确性：永不给用户错误的结果； 让开发者变得更容易：用户输入错误，直接结束（不满足precondition调用）。
  - 健壮性：尽可能保持软件运行而不是总是退出； 让用户变得更容易：出错也可以容忍，程序内部已有容错机制。
  - 正确性倾向于直接报错(error)，健壮性则倾向于容错(fault-tolerance)；
  - 对外的接口，倾向于健壮性；对内的实现，倾向于正确性。
  - Reliability（可靠性） = Robustness + correctness

Problem	健壮性	正确性

浏览器发出包含空格的URL	剥离空白，正常处理请求。	将HTTP 400错误请求错误状态返回给客户端。
视频文件有坏帧	跳过腐败区域到下一个可播放部分。	停止播放，引发“损坏的视频文件”错误
配置文件使用了非法字符	在内部识别最常见的评论前缀，忽略它们。	终止启动时出现“配置错误”错误
奇怪格式的日期输入	尝试针对多种不同的日期格式解析字符串。 将正确的格式呈现给用户。	日期错误无效

如何测量健壮性和正确性

- 外部观察角度：
  - Mean time between failures (MTBF，平均失效间隔时间)：描述了可修复系统的两次故障之间的预期时间，而平均故障时间（MTTF）表示不可修复系统的预期故障时间。
- 内部观察角度：
  - 残余缺陷率：每千行代码中遗留的bug的数量