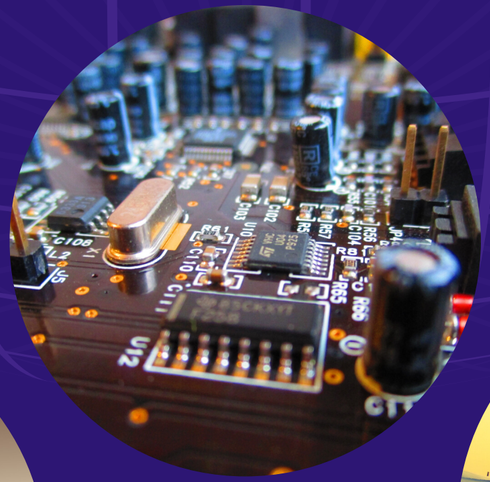
VERIFICAÇÃO DE SOFTWARE EM CONTROLADORES DE VEÍCULOS AÉREOS NÃO-TRIPULADOS

LENNON CHAVES – **SEL SIDIA**

PESQUISA CIENTÍFICA

INTRODUÇÃO/CONCEITO



MOTIVAÇÃO

Problemas relacionados a ***hardware*** podem ser identificados durante a fase de desenvolvimento... e isso evita:

- Prejuízos financeiros
- Problemas com reputação e confiança
- Situações catastróficas como acidentes e perda de vidas

BOEING 737-MAX

TOYOTA (2014)

- Recall de 1.9 milhões de carros (Prius Car)
- Falha de programação no sistema híbrido
- Incidentes prevenidos por verificação formal:
  - ativação de pedal
  - probabilidade de falha em airbags
  - contraexemplo

Ariane 5 (1996)

Problemas com representação numérica

(500 milhões de doláres)

VERIFICAÇÃO DE SOFTWARE

Bounded Model Checking (BMC)

Satisfiability Modulo Theories (SMT)

DSVERIFIER

VERIFICAÇÃO USANDO BOUNDED MODEL CHECKING + TEORIAS DE SATISFATIBILIDADE

Aplicado a controladores digitais

CONTROLADORES DIGITAIS

FUNÇÃO DE TRANSFERÊNCIA (MODELO MATEMÁTICO)

$$H(z) = \frac{B(z)}{A(z)} = \frac{b_0 + b_1 z^{-1} + \ldots + b_M z^{-M}}{a_0 + a_1 z^{-1} + \ldots + a_N z^{-N}}.$$

PROGRAMA EM C

```
#include <dsverifier.h>

digital_system ds = {
    .b = { 0.0096, -0.009 },
    .b_size = 2,
    .a = { 0.02, 0.0 },
    .a_size = 2,
    .sample_time = 0.02
};

implementation impl = {
  .int_bits = 3,
  .frac_bits =  13,
  .max =  1.0,
  .min =  -1.0
  };
```

Infos importantes para um controlador digital:

- **Coeficientes da função de transferência**
- Quantidade de **bits** necessários para controlador (inteiro e fracionário)
- **Limitação** dos valores de **entrada**
- Produz uma **saída** em números, dependendo da propriedade a ser verificada

VANT é um controlador digital

OVERFLOW

estouros aritméticos causando falhas em operações matemáticas

CICLO LIMITE

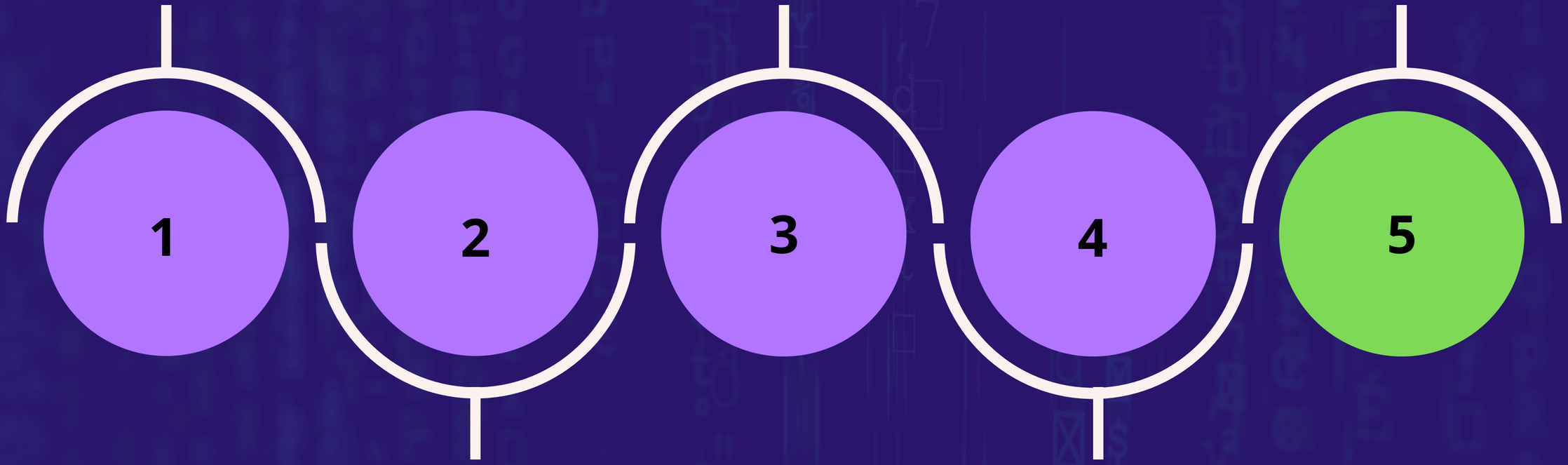
Instabilidade que causa problemas nas hélices do drone

VIGILÂNCIA E SEGURANÇA

CONTROLADOR DIGITAL EM C

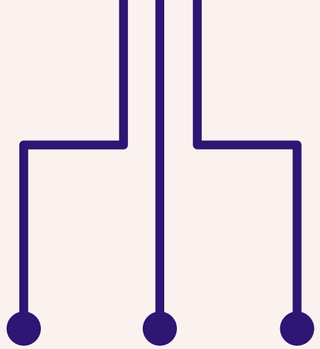
VERIFICAÇÃO PROPRIEDADE

DSVALIDATOR



DSVERIFIER

CONTRAEXEMPLO



DSVERIFIER

PROCESSA O ARQUIVO EM C DO CONTROLADOR

- verifica quantidade de bits
- verifica entrada limitada
- entende o modelo

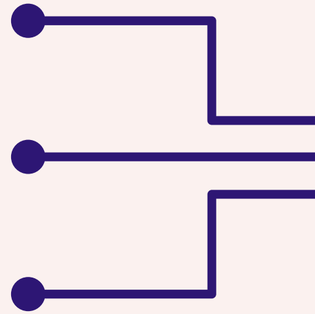
CHAMADA DO MODEL CHECKER (BMC)

- resolve a propriedade através de SMT
- entradas não-determinísticas
- computa a saída
- Falha ou Sucesso
  - Contraexemplo

DSVALIDATOR

- valida se falha é realmente falha

DSVALIDATOR



RESULTADOS DA PESQUISA

- Quantidade de bits usada (8, 16, 32)
- **Integração controle e verificação**!!!
- Quanto maior a quantidade de bits, menos problemas encontrados
- Confirmação de limitação em algoritmos de overflows e corrigidos pela literatura (2017, algoritmos clássicos)
- **5 artigos publicados (IEEE, Science Direct, ACM)**
- **29 trabalhos envolvendo verificação de controladores digitais deade 2013**
  - 1 tese, 3 dissertações, 21 artigos, 4 Iniciações cientificas

SOBRE O GRUPO DE PESQUISA

PROFESSOR LUCAS CORDEIRO (SSV LAB)

ÁREA DE VERIFICAÇÃO DE SOFTWARE

- CONTROLADORES
- IA E IOT
- LOCALIZAÇÃO DE FALHAS
- CUDA
- VANT

UFAM (CETELI E ICOMP)

- CONHECIMENTOS BÁSICOS NECESSÁRIOS:
- BASE EM ALGORITMOS
- BASE EM PROGRAMAÇÃO

APRENDIZADOS
- DESAFIOS
- RESILIÊNCIA
- ARTIGOS DE QUALIDADE
- OPORTUNIDADE INTERNACIONAL

OBRIGADO

CONTATOS

lennon.chaves@sidia.com