



SAFETY-CRITICAL SYSTEMS FROM THE INSIDE

MACIEJ GAJDZICA

MACIEJ GAJDZICA



- senior embedded developer at Solwit
- automotive, railway, medical systems
- ucgosu.pl - blog, YouTube
- Gdańsk Embedded Meetup



 @MaciekGajdzica

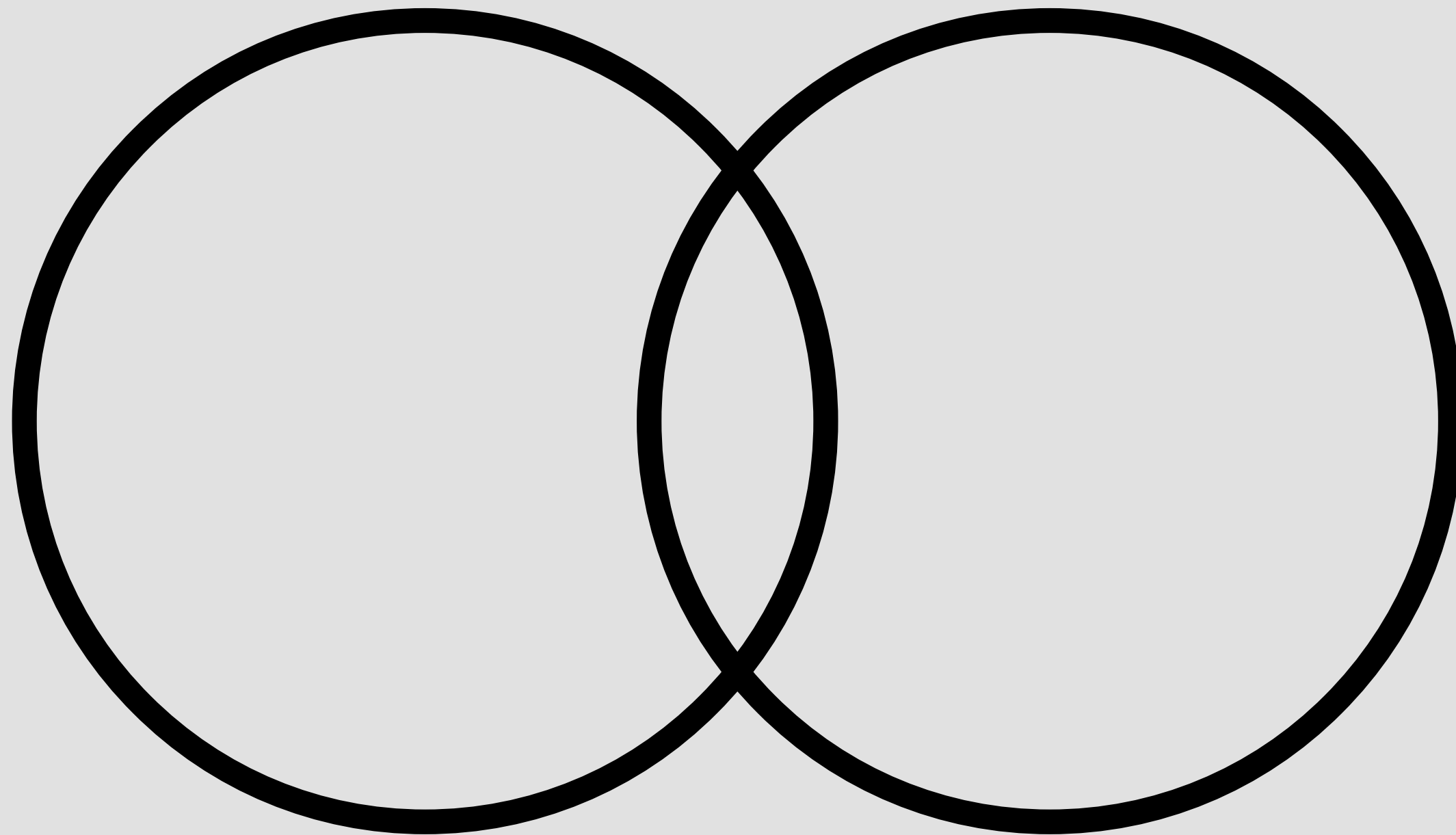
WHAT IS SAFETY CRITICAL SYSTEM?



SYSTEM WHOSE MALFUNCTION CAN LEAD TO:

- death or serious injury of people
- enviromental harm
- loss of expensive equipment

SAFETY VS SECURITY



SAFETY VS RELIABILITY



Safe

better to shut down
than to cause accident

Reliable

always works

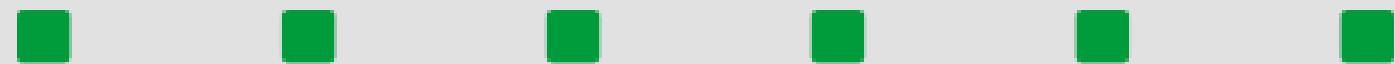


Risk: cutting fingers



Risk: cutting fingers

Solution: working only while button is being pressed



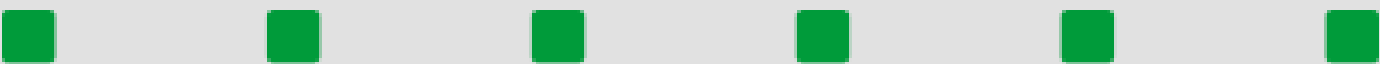
Risk: cutting fingers

Solution: working only while button is being pressed



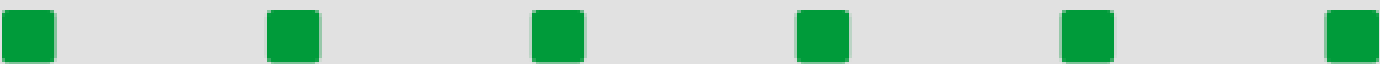


Risk: burning everything



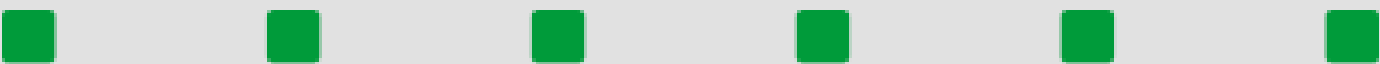
Risk: burning everything

Solution: unable to light
a barbecue



Risk: burning everything

Solution: unable to light
a barbecue



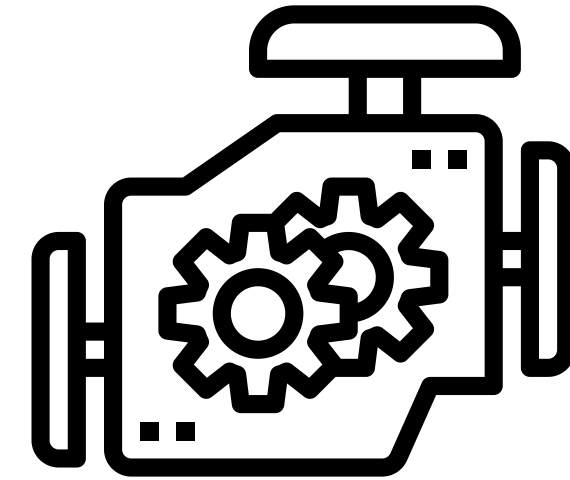


Opening
Mon
Tue-Thu
Fri-Sat
Sunday

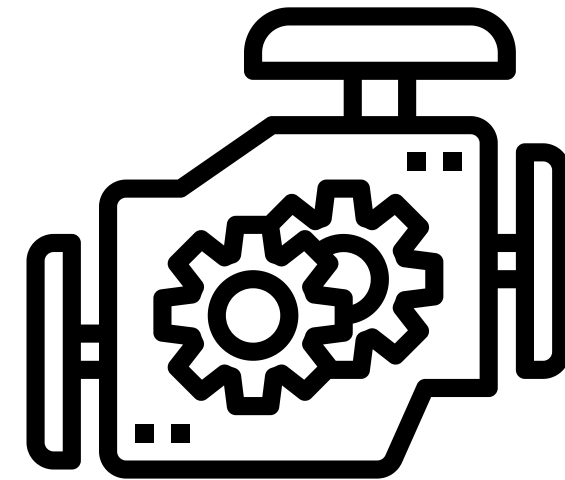
SAFETY INTEGRITY LEVEL (SIL)

Railway	Automotive	Aerospace	Medical	Malfunction may lead to:
SIL 4	ASIL D	DAL A	-	Death of many people
SIL 3	ASIL C	DAL B	Class C	Death of a single person
SIL 2	ASIL B	DAL C	Class B	Severe injury possible
SIL 1	ASIL A	DAL D	Class A	Minor injury possible
SIL 0	-	DAL E	-	No negative effects

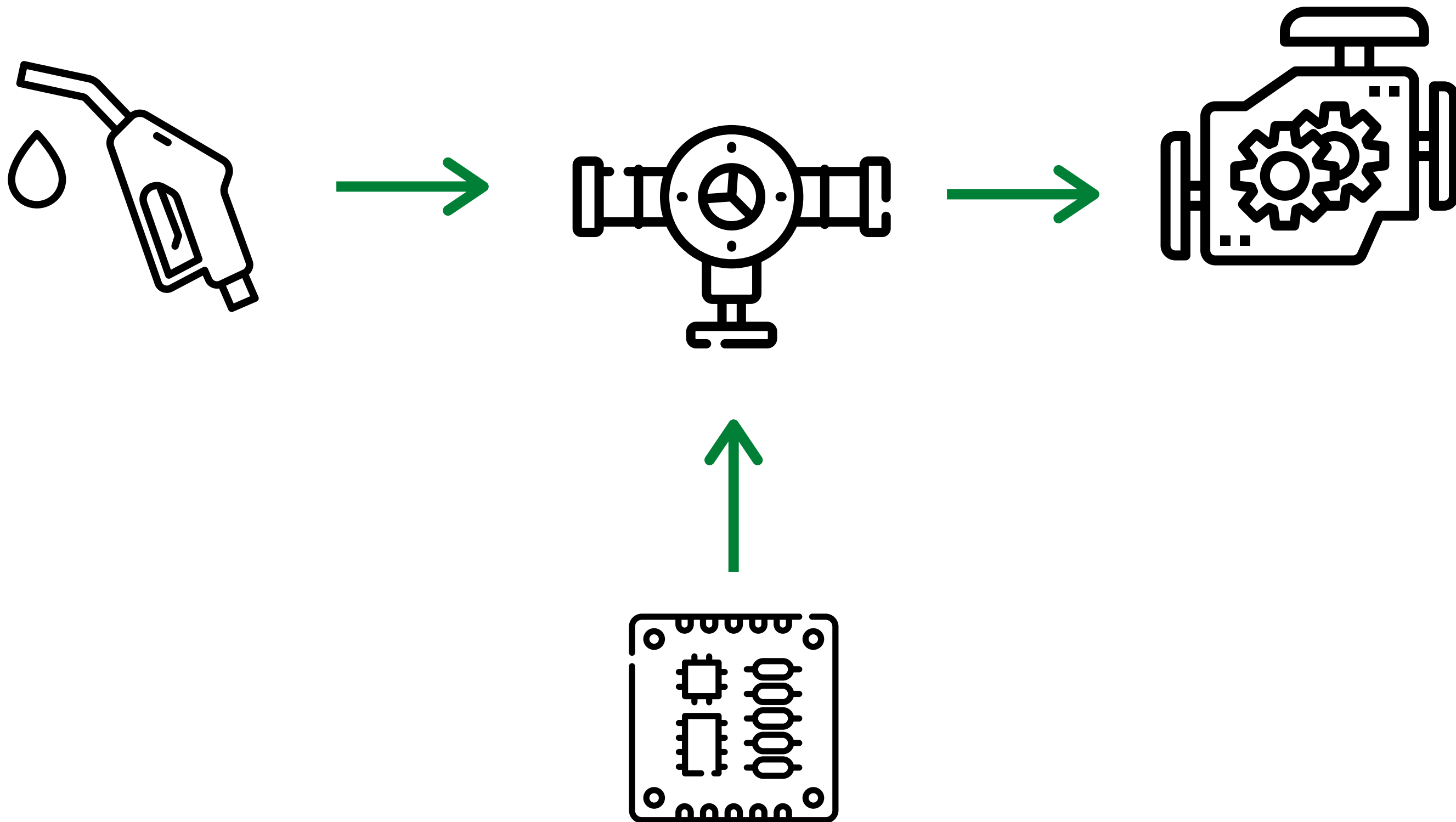
FAIL SAFE



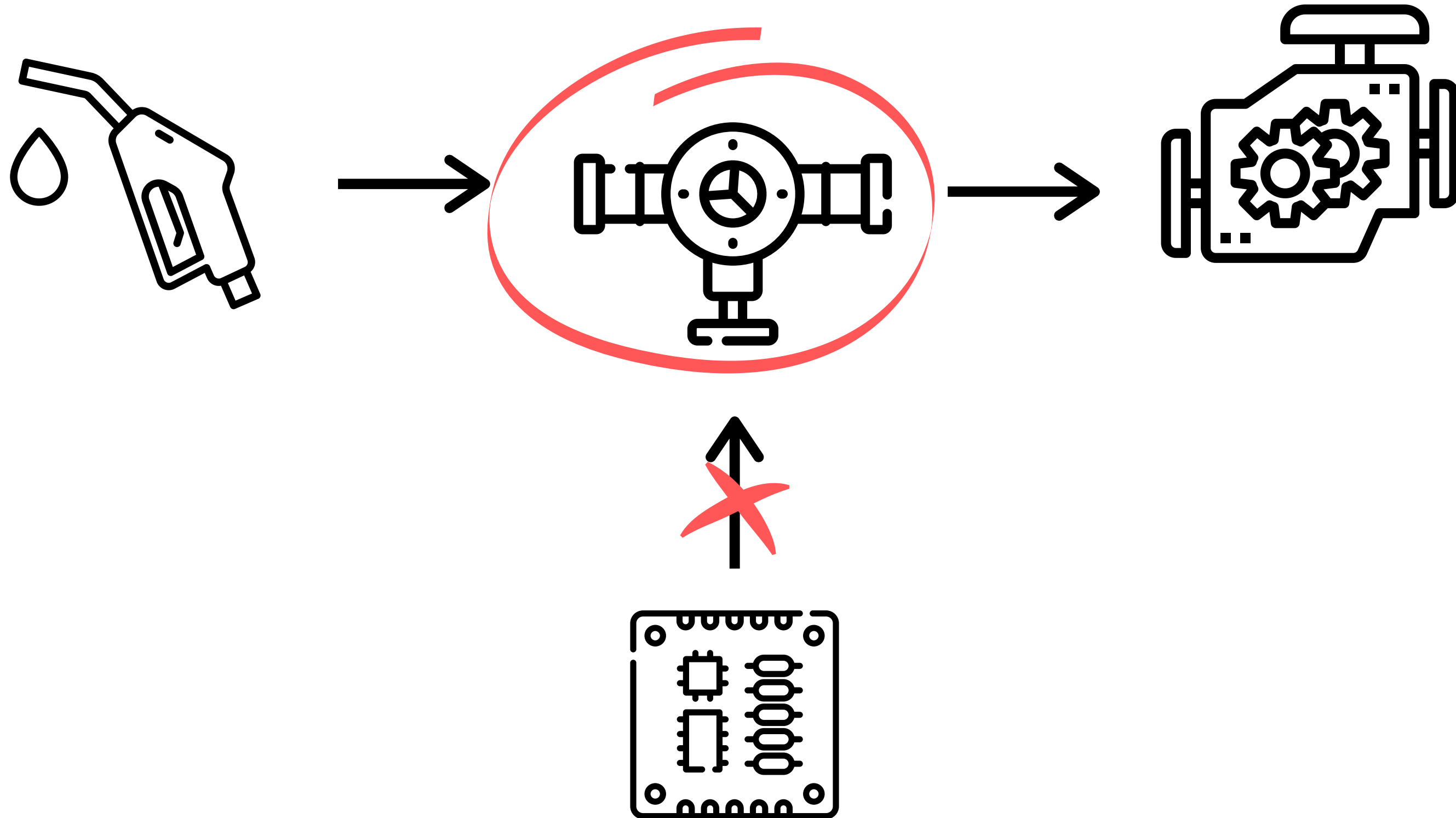
FAIL SAFE



FAIL SAFE



FAIL SAFE

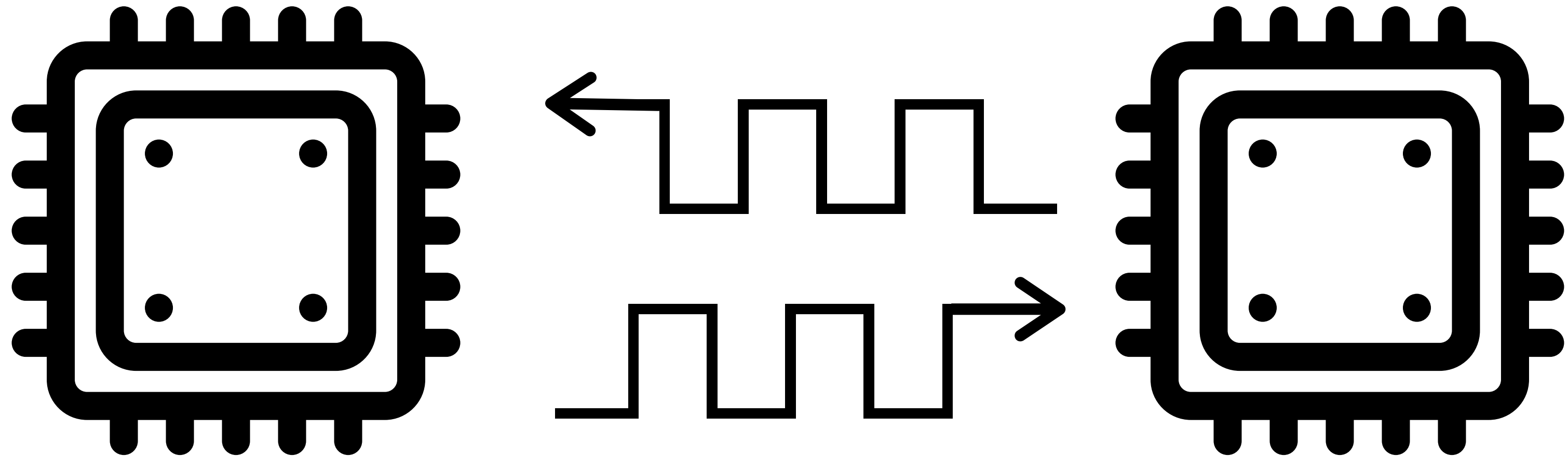




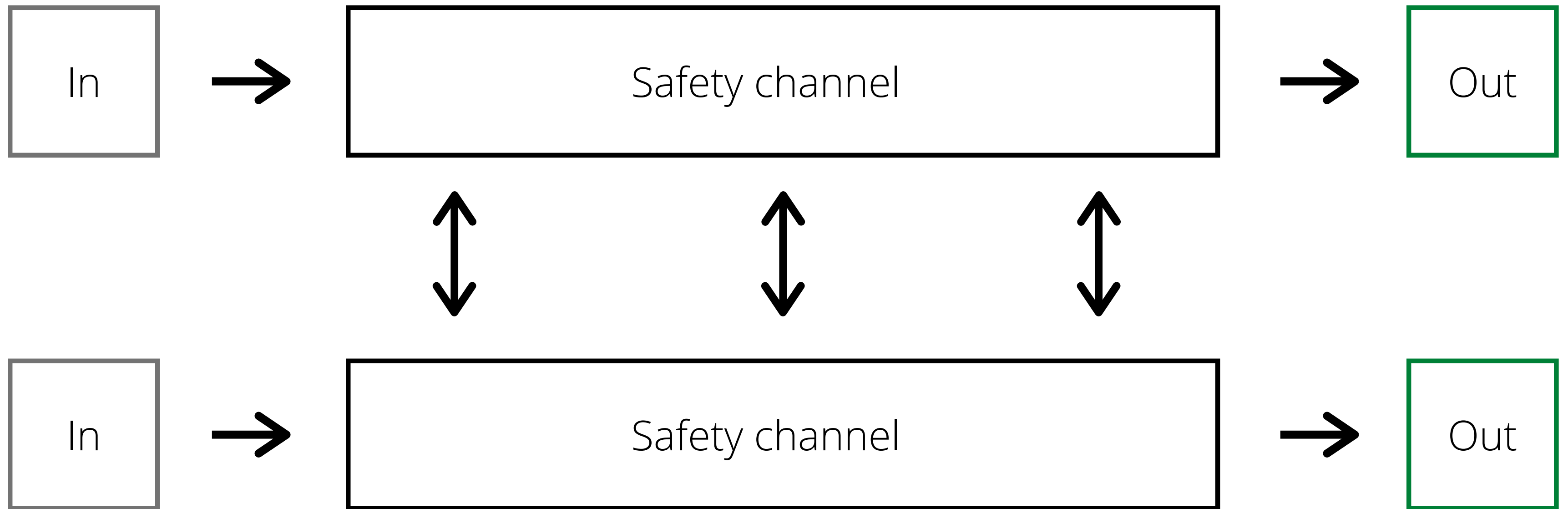
CPU ERRORS

- RAM
- FLASH
- CPU - instructions or registers
- Clock

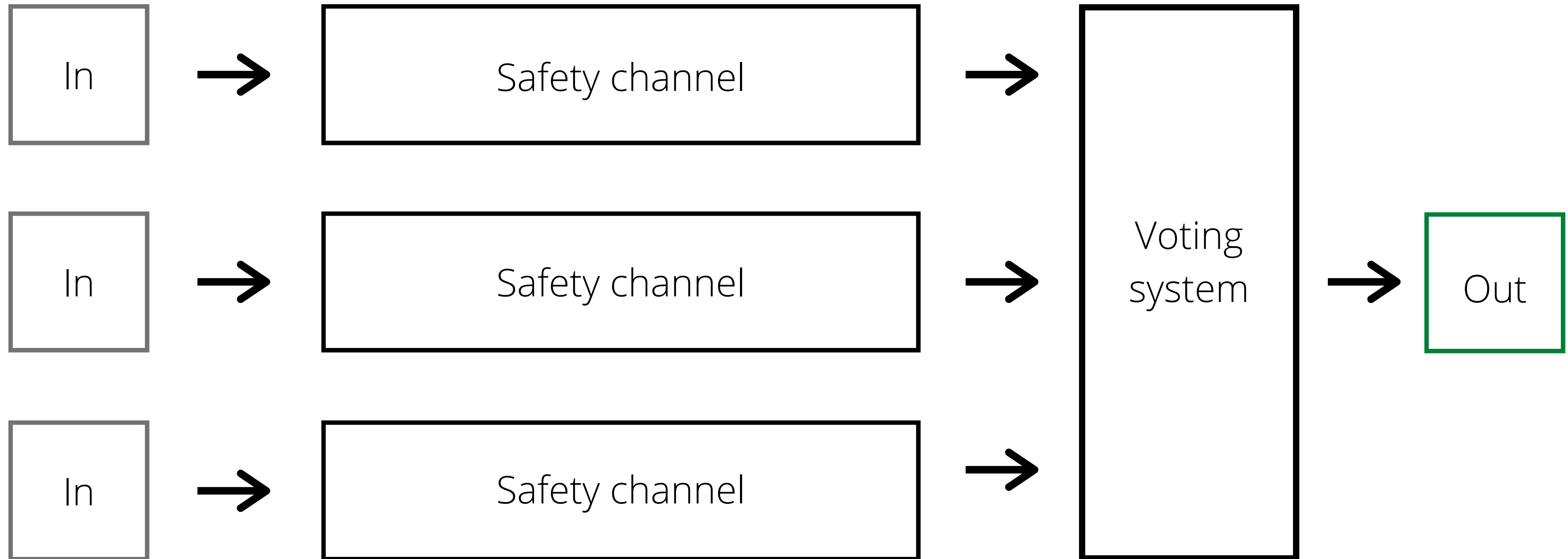
HOW TO DETECT CLOCK FAILURE?



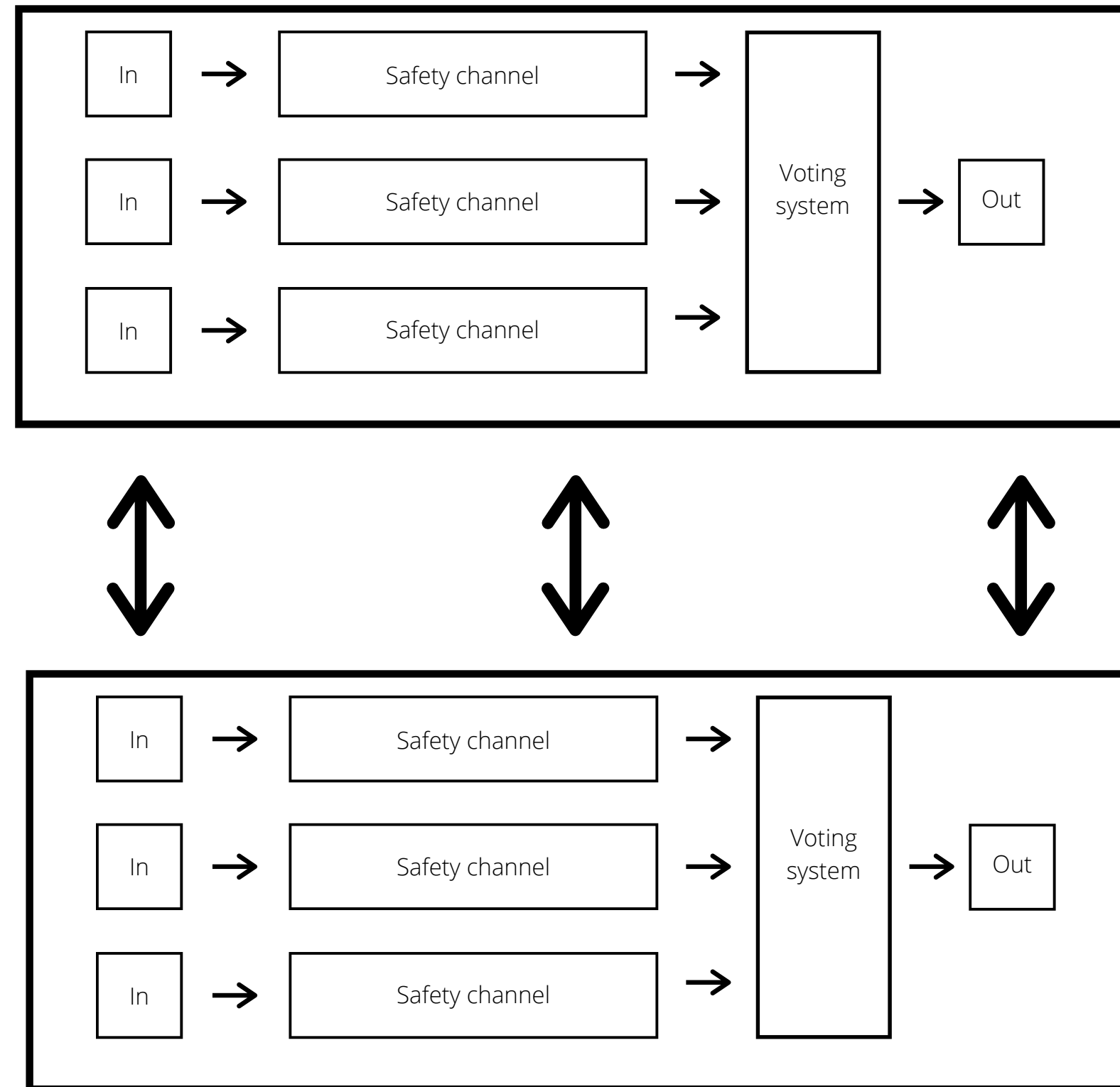
REDUNDANCY



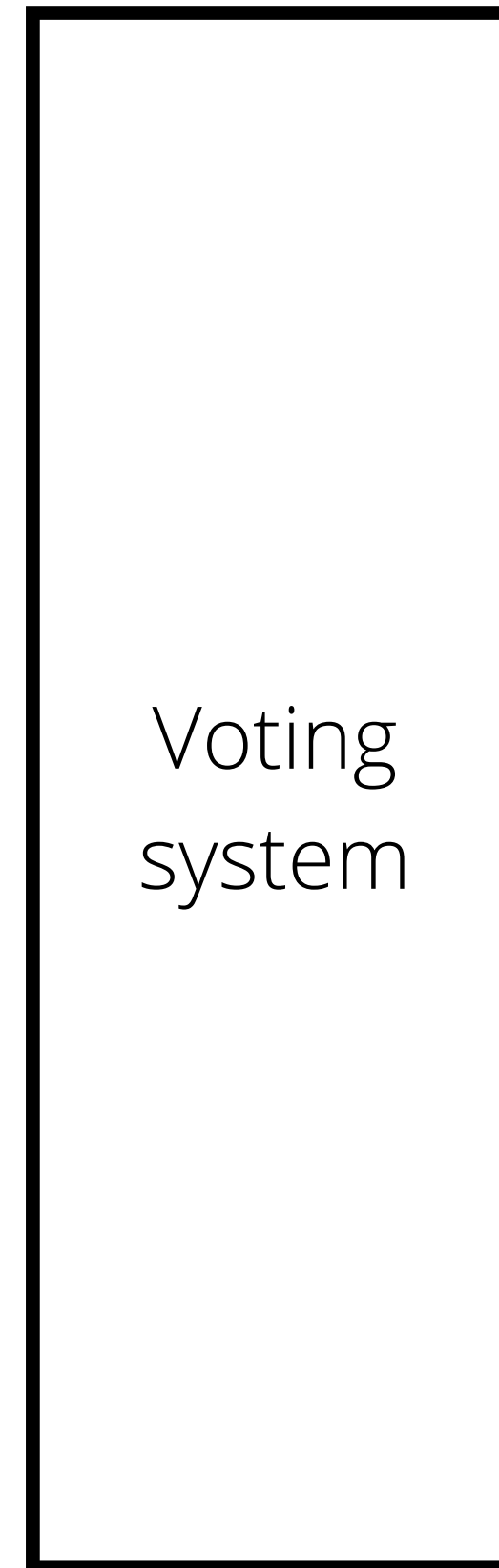
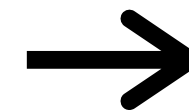
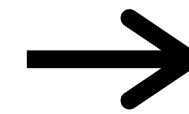
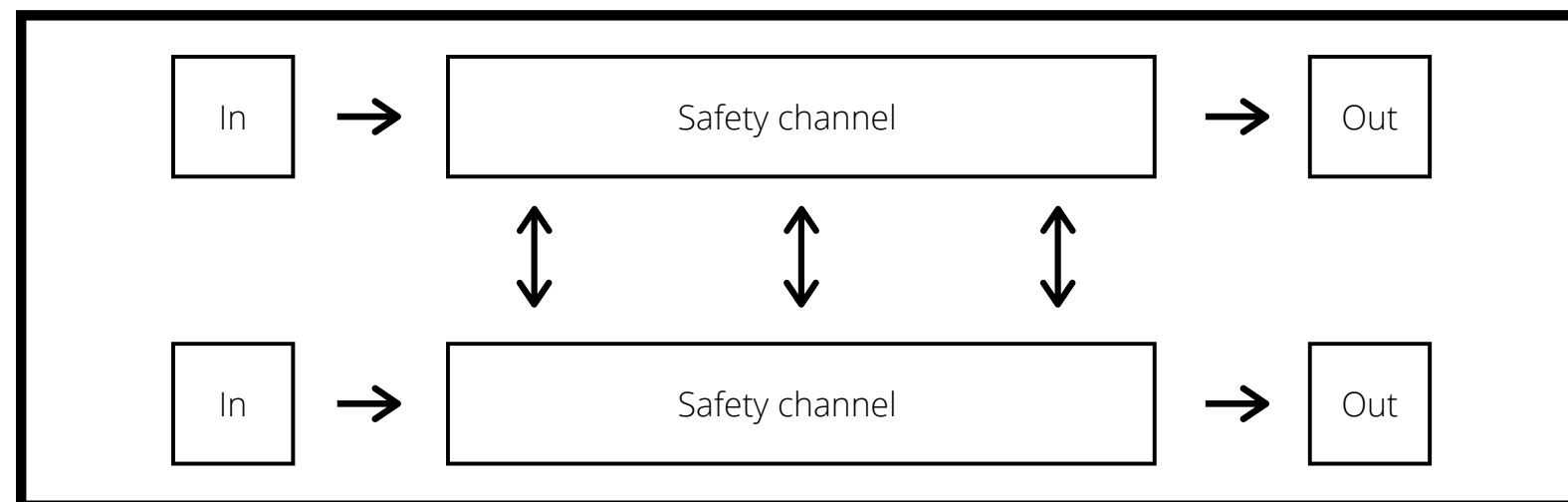
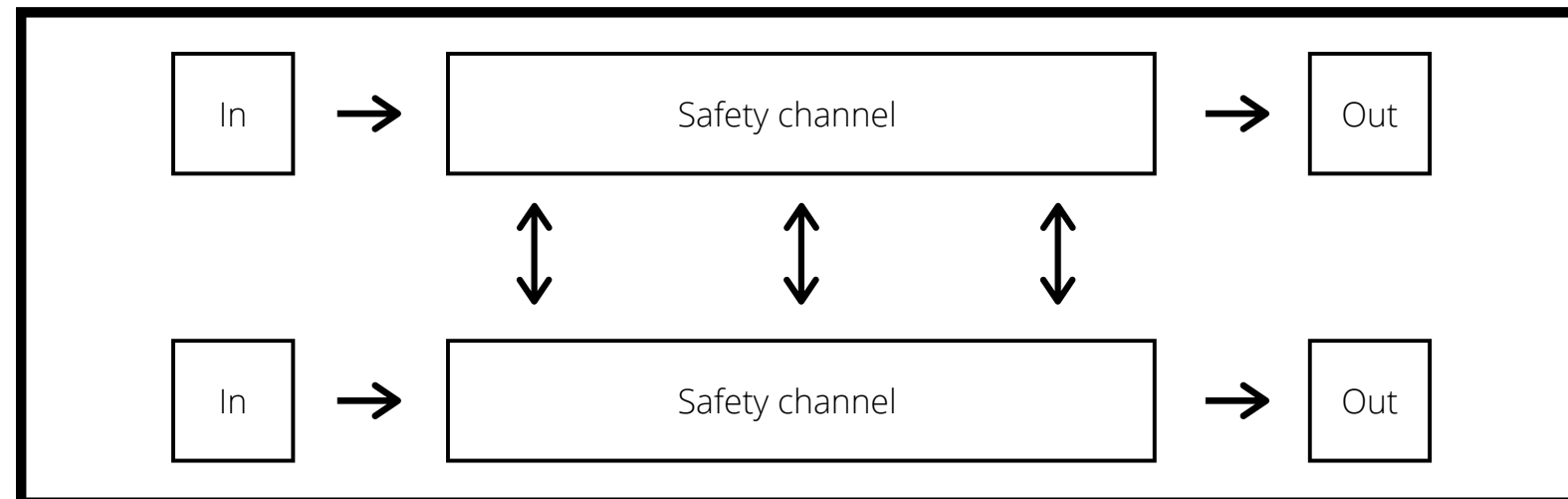
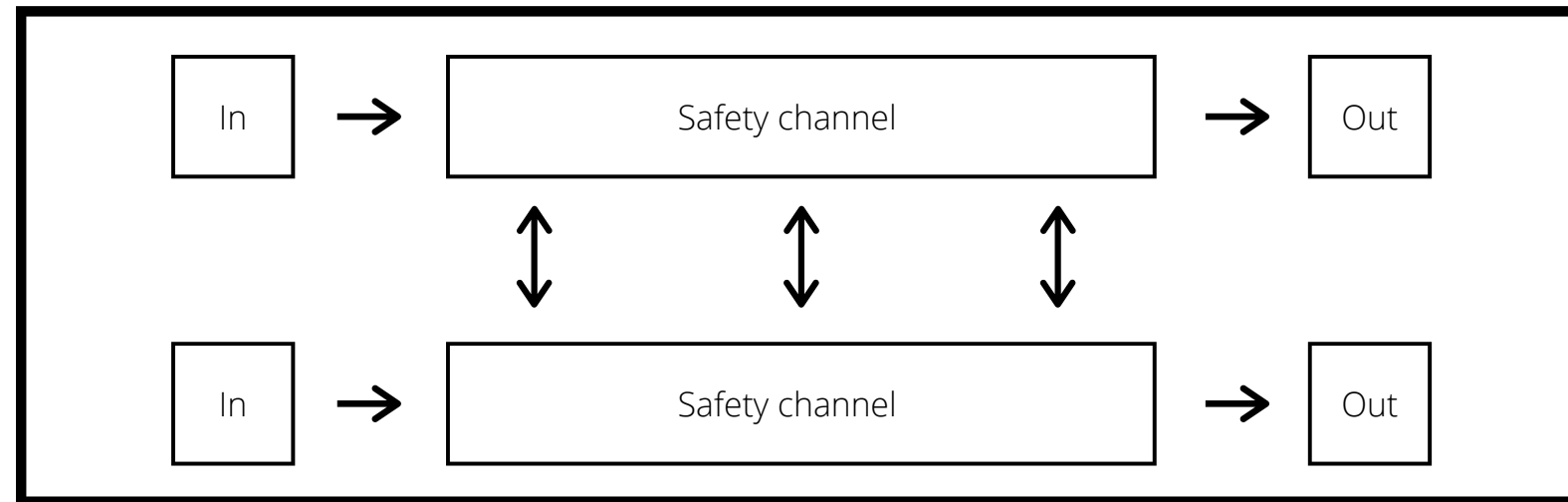
REDUNDANCY



REDUNDANCY



REDUNDANCY





SAFE COMMUNICATION

Defences								
	Sequence number	Timestamp	Timeout	Node IDs	Acknowledge	Handshake	Safety code	Encryption
Threats								
	Repetition	x	x					
	Deletion	x						
	Insertion	x			x	x	x	
	Resequence	x	x					
	Corruption						x	x
	Delay		x	x				
	Masquerade					x	x	x

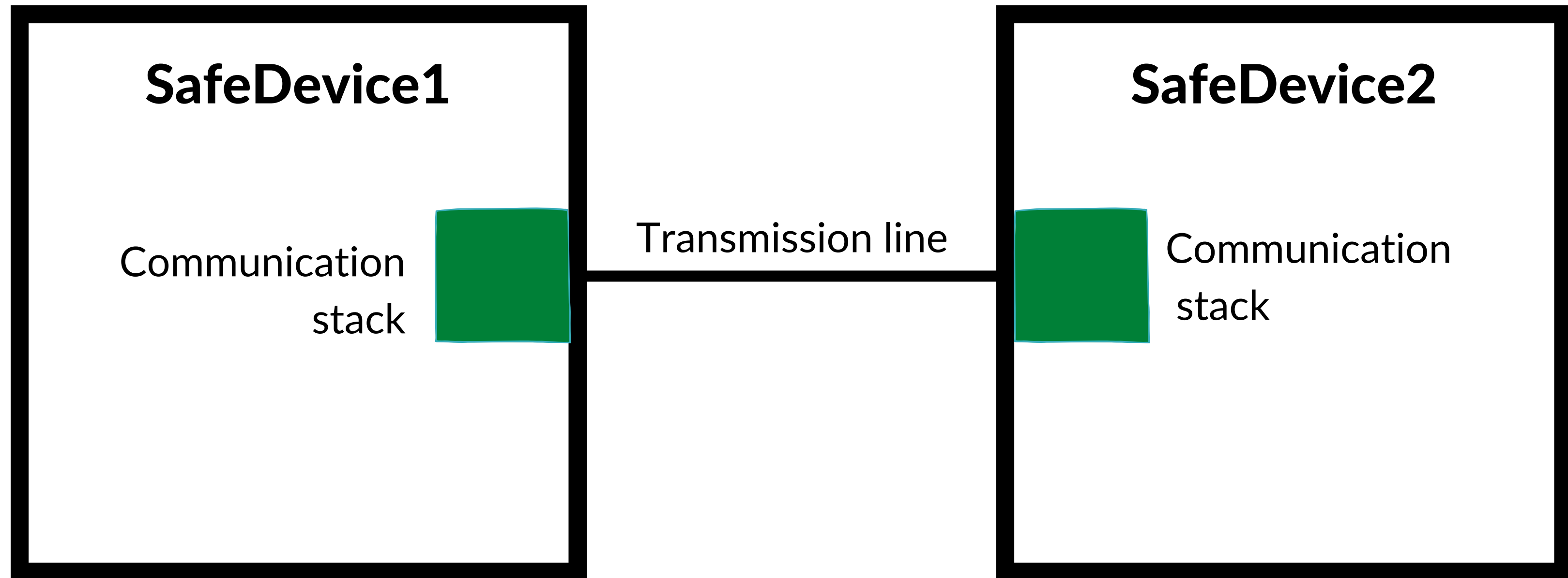
SAFE COMMUNICATION

Network category	Threats						
	Repetition	Deletion	Insertion	Resequencing	Corruption	Delay	Masquerade
1	+	+	+	+	++	+	-
2	++	++	++	+	++	++	-
3	++	++	++	++	++	++	++

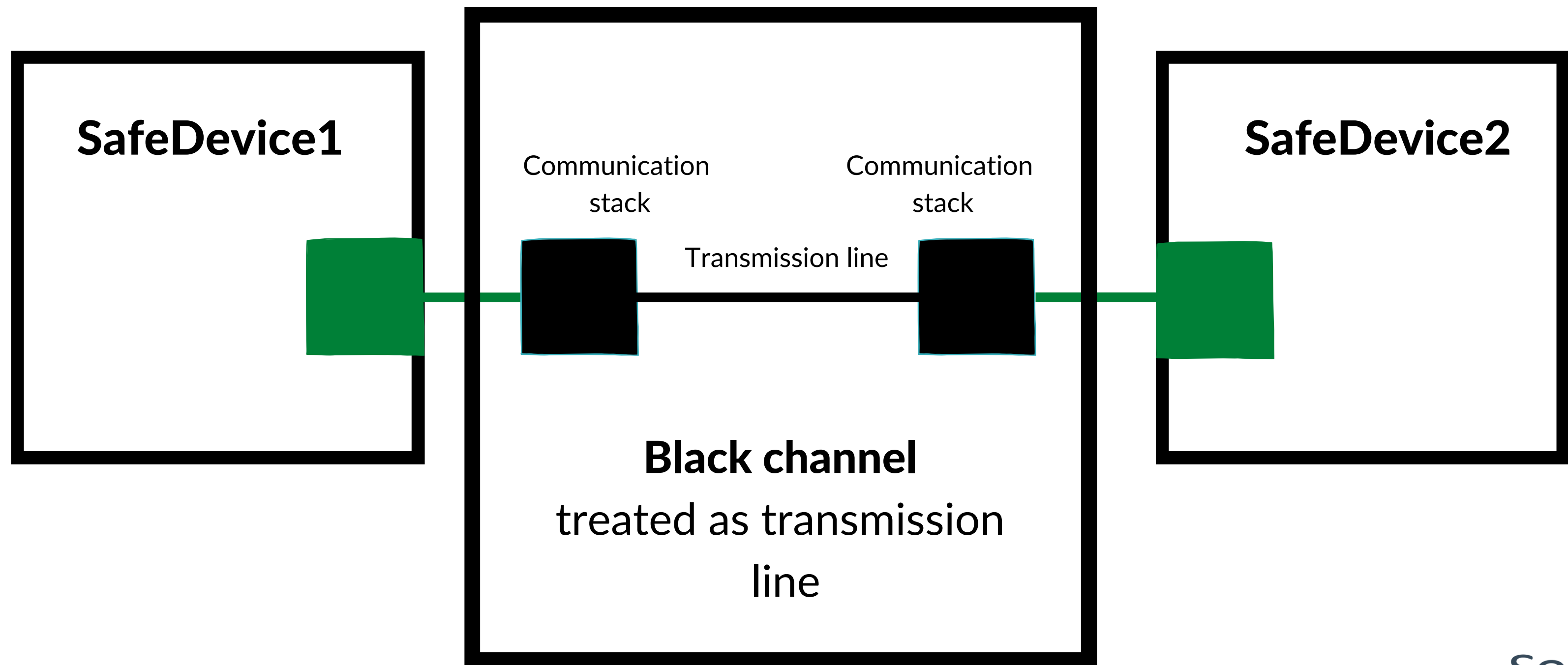
Legend:

- Threat can be neglected
- + Rare, weak countermeasures sufficient
- ++ Threat exists, strong countermeasures required

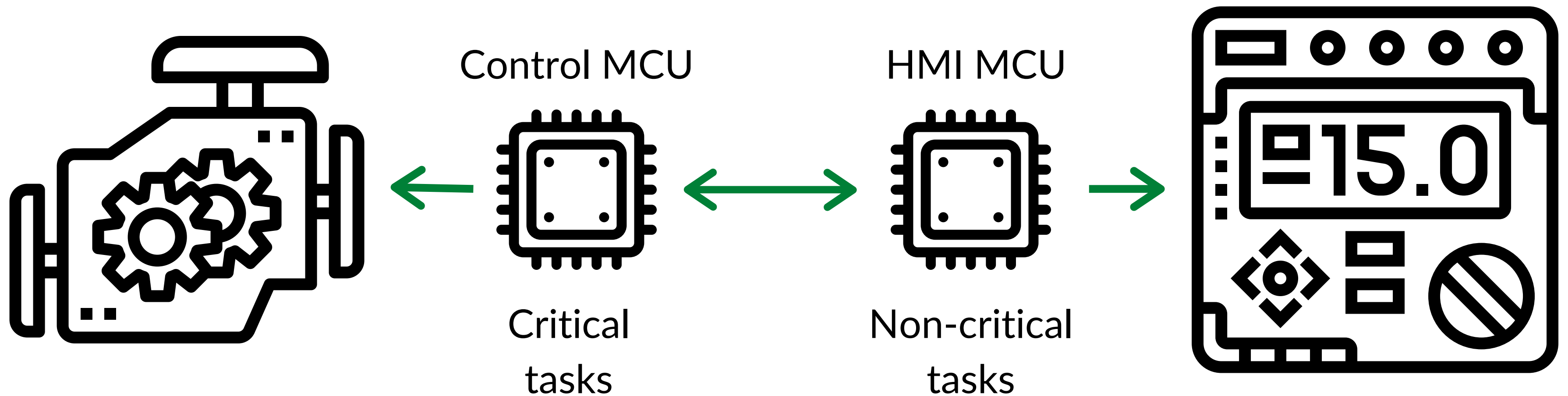
PROBLEM



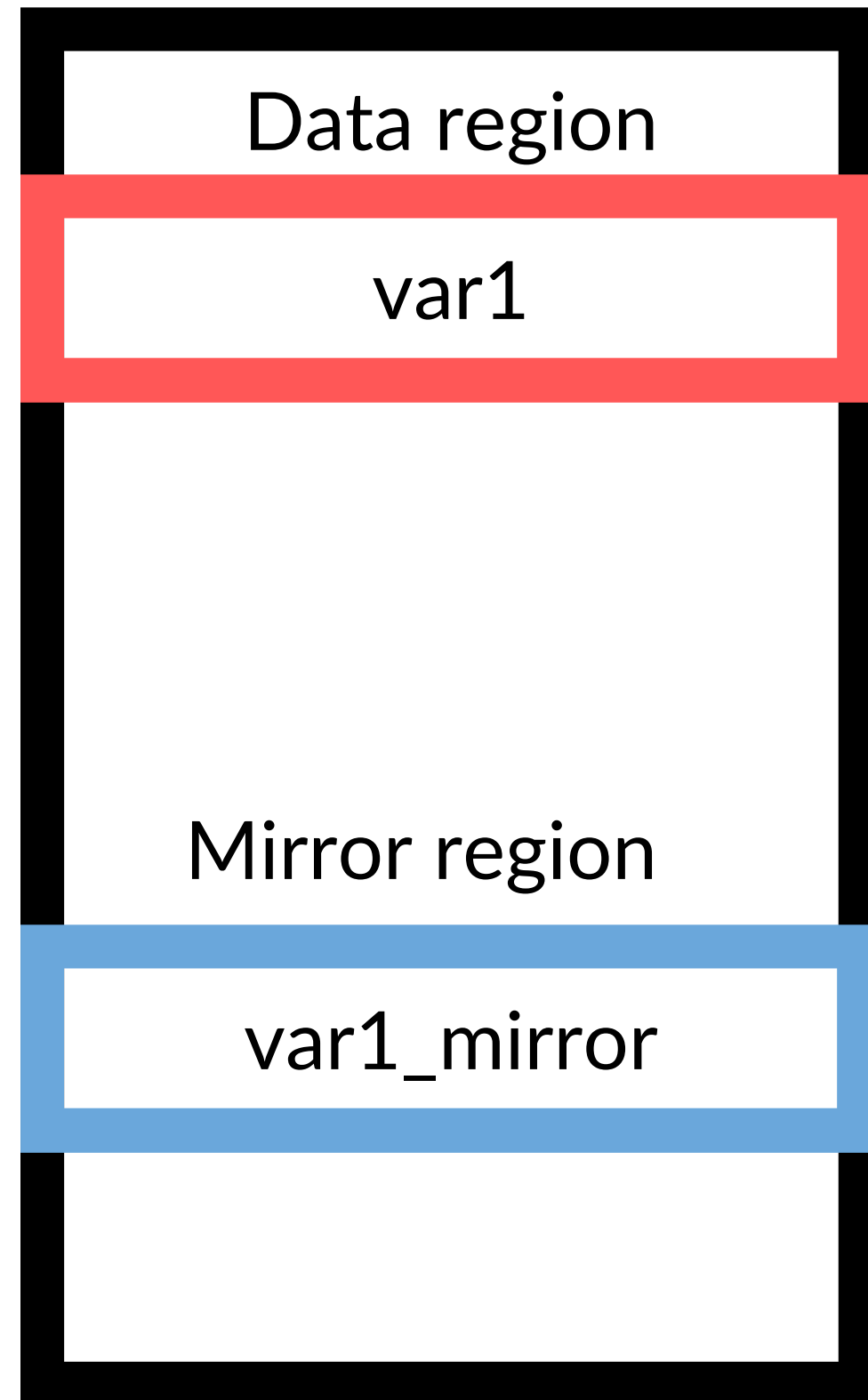
SOLUTION



MIXED CRITICALITY



DATA CORRUPTION



Invariant:

$$\text{var1} \wedge \text{var1_mirror} = 0xFFFFFFFF$$

```
uint32_t tick_cnt CRITICAL_DATA;  
uint32_t tick_cnt_inv CRITICAL_DATA_MIRROR;  
  
/* Verify TickCounter integrity */  
if ((tick_cnt ^ tick_cnt_inv) == 0xFFFFFFFFFuL)  
{  
    tick_cnt++;  
    tick_cnt_inv = ~tick_cnt;  
  
if (tick_cnt >= SYSTICK_10ms)  
{  
    tick_cnt = 0u;  
    tick_cnt_inv = 0xFFFFFFFFFuL;  
}  
}
```



```
struct safe_var
{
    uint32_t * const value;
    uint32_t * const value_inv;
};
```

```
void safe_var_init(const struct safe_var *var);
uint32_t safe_var_get(const struct safe_var *var);
void safe_var_set(const struct safe_var *var,
                  uint32_t val);
```

```
uint32_t tick_cnt CRITICAL_DATA;
uint32_t tick_cnt_inv CRITICAL_DATA_MIRROR;
```

```
const struct safe_var safe_tick_cnt =
    {&tick_cnt, &tick_cnt_inv};
```

```
uint32_t tick_val = safe_var_get(&safe_tick_cnt);
safe_var_set(&safe_tick_cnt, tick_val++);
```



```
struct safe_var
{
    uint32_t * const value;
    uint32_t * const value_inv;
};
```

```
void safe_var_init(const struct safe_var *var);
uint32_t safe_var_get(const struct safe_var *var);
void safe_var_set(const struct safe_var *var,
                  uint32_t val);
```

```
uint32_t tick_cnt CRITICAL_DATA;
uint32_t tick_cnt_inv CRITICAL_DATA_MIRROR;
```

```
const struct safe_var safe_tick_cnt =
    {&tick_cnt, &tick_cnt_inv};
```

```
uint32_t tick_val = safe_var_get(&safe_tick_cnt);
safe_var_set(&safe_tick_cnt, tick_val++);
```

```
struct safe_var
{
    uint32_t * const value;
    uint32_t * const value_inv;
};

void safe_var_init(const struct safe_var *var);
uint32_t safe_var_get(const struct safe_var *var);
void safe_var_set(const struct safe_var *var,
                  uint32_t val);

uint32_t tick_cnt CRITICAL_DATA;
uint32_t tick_cnt_inv CRITICAL_DATA_MIRROR;

const struct safe_var safe_tick_cnt =
    {&tick_cnt, &tick_cnt_inv};

uint32_t tick_val = safe_var_get(&safe_tick_cnt);
safe_var_set(&safe_tick_cnt, tick_val++);
```



```
struct safe_var
{
    uint32_t * const value;
    uint32_t * const value_inv;
};

void safe_var_init(const struct safe_var *var);
uint32_t safe_var_get(const struct safe_var *var);
void safe_var_set(const struct safe_var *var,
                  uint32_t val);

uint32_t tick_cnt CRITICAL_DATA;
uint32_t tick_cnt_inv CRITICAL_DATA_MIRROR;

const struct safe_var safe_tick_cnt =
    {&tick_cnt, &tick_cnt_inv};

uint32_t tick_val = safe_var_get(&safe_tick_cnt);
safe_var_set(&safe_tick_cnt, tick_val++);
```



```

struct safe_var
{
    uint32_t * const value;
    uint32_t * const value_inv;
};

void safe_var_init(const struct safe_var *var);
uint32_t safe_var_get(const struct safe_var *var);
void safe_var_set(const struct safe_var *var,
                  uint32_t val);

uint32_t tick_cnt CRITICAL_DATA;
uint32_t tick_cnt_inv CRITICAL_DATA_MIRROR;

const struct safe_var safe_tick_cnt =
    {&tick_cnt, &tick_cnt_inv};

uint32_t tick_val = safe_var_get(&safe_tick_cnt);
safe_var_set(&safe_tick_cnt, tick_val++);

```

LANGUAGES





ADA

```
type My_Int is range -1 .. 20;
```

ADA

```
type My_wrapping_int is mod 2 ** 5;
```

ADA

```
type Item is range 0 .. 1000;  
type Index is range 0 .. 4;  
type My_Array is array (Index) of Item;
```

ADA

```
type Item is range 0 .. 1000;  
type Index is range 1 .. 5;  
type My_Array is array (Index) of Item;
```


ADA

```
type Item is range 0 .. 1000;  
type Index is range 11 .. 15;  
type My_Array is array (Index) of Item;
```

ADA

```
procedure Illegal_Example is
  -- Declare two different floating point types
  type Meters is new Float;
  type Miles is new Float;

  Dist_Imperial : Miles;

  -- Declare a constant
  Dist_Metric : constant Meters := 100.0;
begin
  -- Not correct: types mismatch
  Dist_Imperial := (Dist_Metric * 1609.0) / 1000.0;
  Put_Line (Miles'Image (Dist_Imperial));
end Illegal_Example;
```

ADACORE



SPARK Ada for the MISRA C Developer
Yannick Moy



AdaCore Technologies for Cyber Security
Roderick Chapman & Yannick Moy



Ada for the C++ or Java Developer
Quentin Ochem



AdaCore Technologies for DO-178C / ED-12C
Frédéric Pothon & Quentin Ochem



AdaCore Technologies for CENELEC EN 50128:2011
Jean-Louis Boulanger & Quentin Ochem



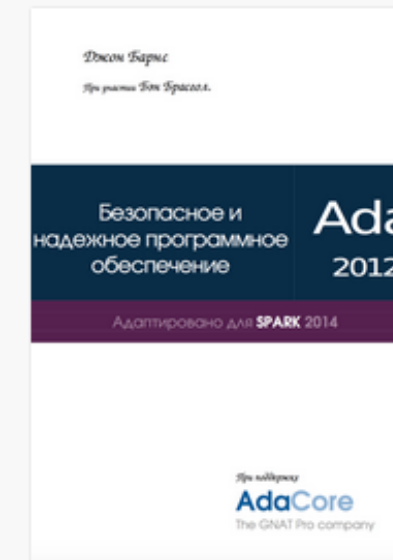
Implementation Guidance for the Adoption of SPARK



Embedded SPARK and Ada Use Cases
Multiple Authors



Safe and Secure Software - An Invitation to Ada 2012
John Barnes

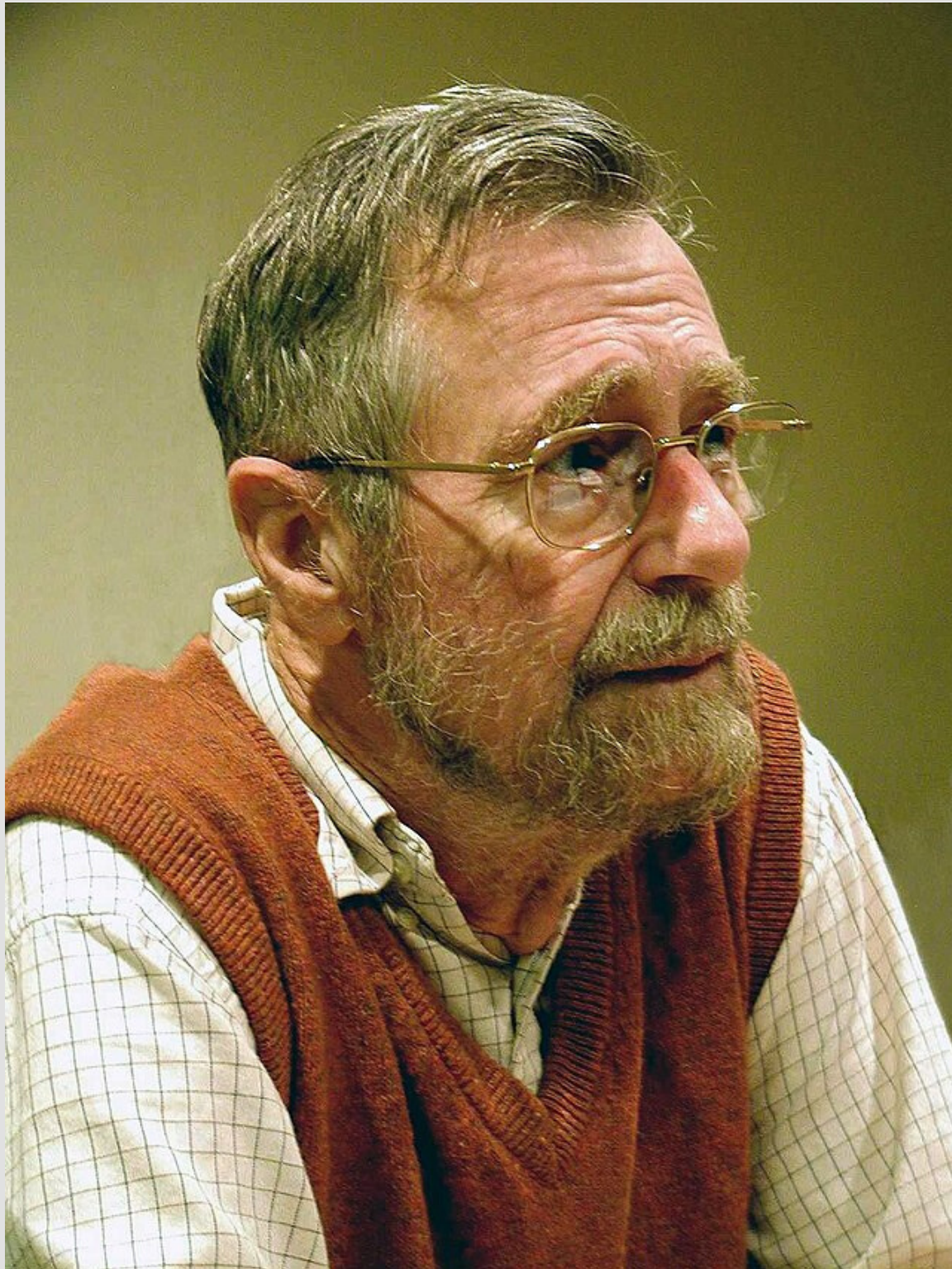


Safe and Secure Software Updated for SPARK (Russian Translation)



Dissimilar tools: Use cases and impact on tool qualification level

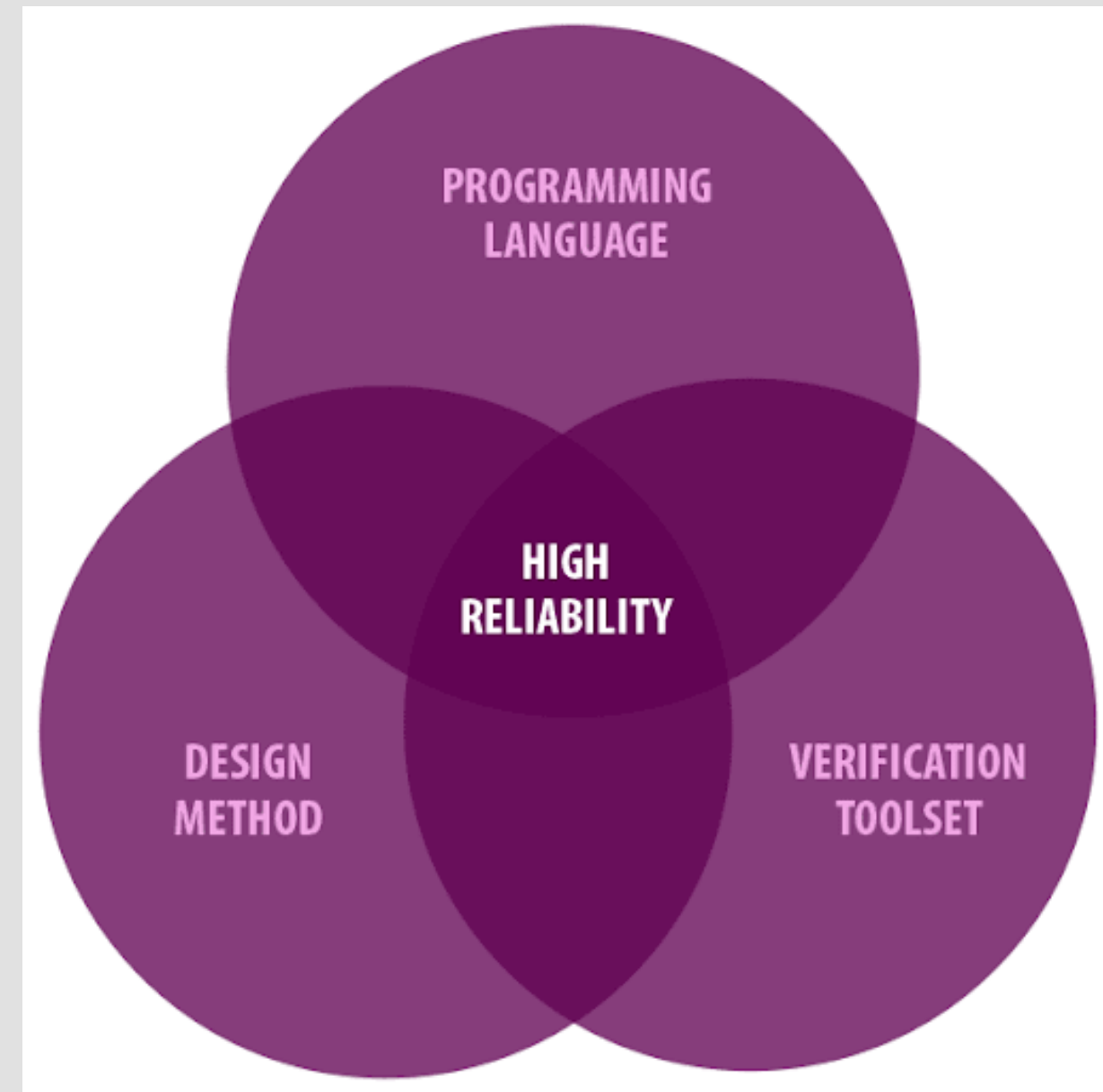
FORMAL PROOF



“Program testing can be used to show the presence of bugs, but never to show their absence!”

EDSGER DIJKSTRA

ADA SPARK



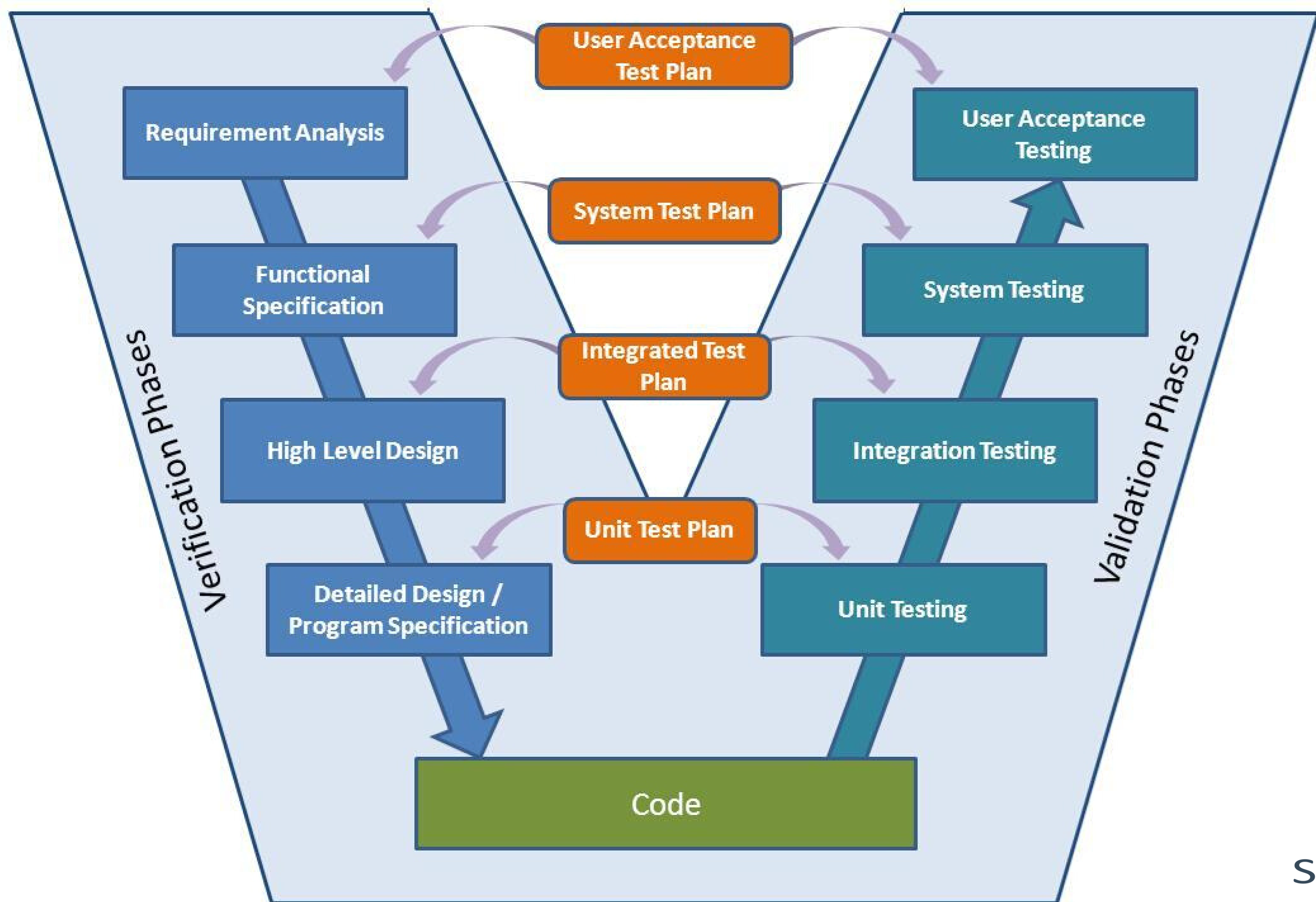
SPARK2014

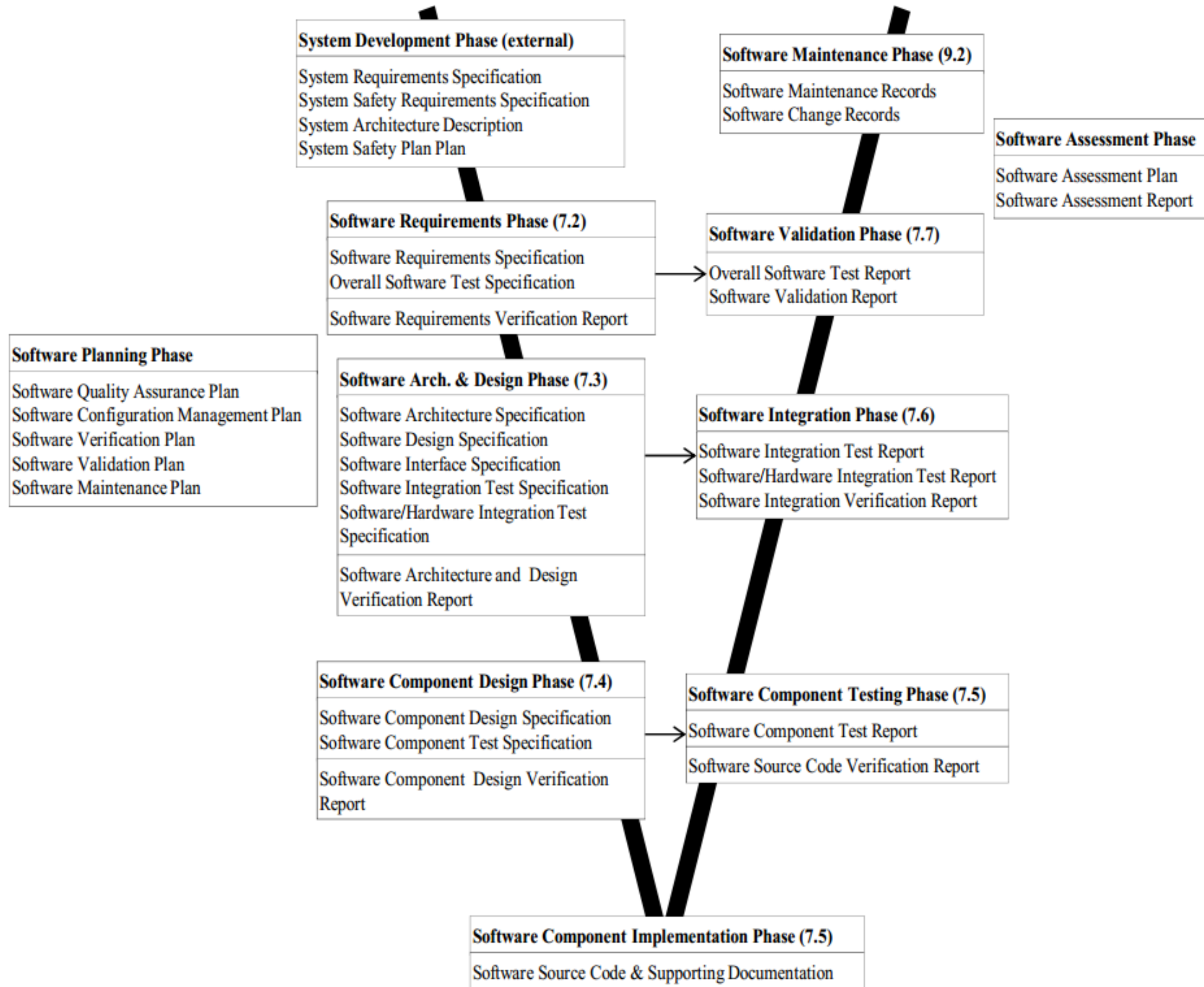


LANGUAGE SUBSETS

- MISRA C
- AUTOSAR C++









EFFECTIVE DOCUMENTATION

- part of code review
- cannot merge when not updated
- documentation first



VERSION MANAGEMENT

- version for every binary
- version for every PCB
- version for every bundle





BUT ALSO...

- version of compiler
- version of OS
- version of HW debugger
- version of build system
- version of config generator
- version of every tool used

YOU MUST BE ABLE TO REBUILD
ORIGINAL BINARY FROM SOURCE
FOR THE WHOLE PRODUCT
LIFETIME

...EVEN IF PRODUCT LIFETIME
IS 20 YEARS

Workspace 'mymfc14': 1 project

mymfc14 files

Source Files

MainFrm.cpp

mymfc14.cpp

mymfc14.rc

mymfc14Doc.cpp

mymfc14View.cpp

Persist.cpp

StdAfx.cpp

Header Files

MainFrm.h

mymfc14.h

mymfc14Doc.h

mymfc14View.h

Persist.h

Resource.h

StdAfx.h

Resource Files

Clas...

Res...

FileV...

mymfc14View.cpp

```
// mymfc14View.cpp : implementation of the CMymfc14View class
//
#include "stdafx.h"
#include "mymfc14.h"

#include "mymfc14Doc.h"
#include "mymfc14View.h"

#ifdef _DEBUG
#define new DEBUG_NEW
#undef THIS_FILE
static char THIS_FILE[] = __FILE__;
#endif

//////////////////////
// CMymfc14View

IMPLEMENT_DYNCREATE(CMymfc14View, CView)

BEGIN_MESSAGE_MAP(CMymfc14View, CView)
    //{{AFX_MSG_MAP(CMymfc14View)
    // NOTE - the ClassWizard will add and remove messages here.
    // DO NOT EDIT what you see in this block!
    //{{AFX_MSG_MAP
END_MESSAGE_MAP()
```

DEBUG TOOLBAR

ASSEMBLY CODE

CALL STACK WINDOW

Disassembly

23: {

5F4334A0 push ebp

5F4334A1 mov ebp, esp

5F4334A3 sub esp, 0Ch

5F4334A6 push

5F4334A7 push

5F4334A8 push edi

24: ASSERT(hPrevInstance == NULL);

5F4334A9 cmp dword ptr [hPrevInstance], 0

5F4334B0 jnz 5F4334B4

5F4334B1 jmp 5F4334B4

5F4334B2

5F4334B3

5F4334B4

5F4334B5

5F4334B6

5F4334B7

5F4334B8

5F4334B9

5F4334BA

5F4334BB

5F4334BC

5F4334BD

5F4334BE

5F4334BF

5F4334C0

5F4334C1

5F4334C2

5F4334C3

5F4334C4

5F4334C5

5F4334C6

5F4334C7

5F4334C8

5F4334C9

5F4334CA

5F4334CB

5F4334CC

5F4334CD

5F4334CE

5F4334CF

5F4334D0

5F4334D1

5F4334D2

5F4334D3

5F4334D4

5F4334D5

5F4334D6

5F4334D7

5F4334D8

5F4334D9

5F4334DA

5F4334DB

5F4334DC

5F4334DD

5F4334DE

5F4334DF

5F4334E0

5F4334E1

5F4334E2

5F4334E3

5F4334E4

5F4334E5

5F4334E6

5F4334E7

5F4334E8

5F4334E9

5F4334EA

5F4334EB

5F4334EC

5F4334ED

5F4334EE

5F4334EF

5F4334F0

5F4334F1

5F4334F2

5F4334F3

5F4334F4

5F4334F5

5F4334F6

5F4334F7

5F4334F8

5F4334F9

5F4334FA

5F4334FB

5F4334FC

5F4334FD

5F4334FE

5F4334FF

5F433500

5F433501

5F433502

5F433503

5F433504

5F433505

5F433506

5F433507

5F433508

5F433509

5F43350A

5F43350B

5F43350C

5F43350D

5F43350E

5F43350F

5F433510

5F433511

5F433512

5F433513

5F433514

5F433515

5F433516

5F433517

5F433518

5F433519

5F43351A

5F43351B

5F43351C

5F43351D

5F43351E

5F43351F

5F433520

5F433521

5F433522

5F433523

5F433524

5F433525

5F433526

5F433527

5F433528

5F433529

5F43352A

5F43352B

5F43352C

5F43352D

5F43352E

5F43352F

5F433530

5F433531

5F433532

5F433533

5F433534

5F433535

5F433536

5F433537

5F433538

5F433539

5F43353A

5F43353B

5F43353C

5F43353D

5F43353E

5F43353F

5F433540

5F433541

5F433542

5F433543

5F433544

5F433545

5F433546

5F433547

5F433548

5F433549

5F43354A

5F43354B

5F43354C

5F43354D

5F43354E

5F43354F

5F433550

5F433551

5F433552

5F433553

5F433554

5F433555

5F433556

5F433557

5F433558

5F433559

5F43355A

5F43355B

5F43355C

5F43355D

5F43355E

5F43355F

5F433560

5F433561

5F433562

5F433563

5F433564

5F433565

5F433566

5F433567

5F433568

5F433569

5F43356A

5F43356B

5F43356C

5F43356D

5F43356E

5F43356F

5F433570

5F433571

5F433572

5F433573

5F433574

5F433575

5F433576

5F433577

5F433578

5F433579

5F43357A

5F43357B

5F43357C

5F43357D

5F43357E

5F43357F

5F433580

5F433581

5F433582

5F433583

5F433584

5F433585

5F433586

5F433587

5F433588

5F433589

5F43358A

5F43358B

5F43358C

5F43358D

5F43358E

5F43358F

5F433590

5F433591

5F433592

5F433593

5F433594

5F433595

5F433596

5F433597

5F433598

5F433599

5F43359A

5F43359B

5F43359C

5F43359D

5F43359E

5F43359F

5F4335A0

5F4335A1

5F4335A2

5F4335A3

5F4335A4

5F4335A5

5F4335A6

5F4335A7

5F4335A8

5F4335A9

5F4335AA

5F4335AB

5F4335AC

5F4335AD

5F4335AE

5F4335AF

5F4335B0

5F4335B1

5F4335B2

5F4335B3

5F4335B4

5F4335B5

5F4335B6

5F4335B7

5F4335B8

5F4335B9

5F4335BA

5F4335BB

5F4335BC

5F4335BD

5F4335BE

5F4335BF

5F4335C0

5F4335C1

5F4335C2

5F4335C3

5F4335C4

5F4335C5

5F4335C6

5F4335C7

5F4335C8

5F4335C9

5F4335CA

5F4335CB

5F4335CC

5F4335CD

5F4335CE

5F4335CF

5F4335D0

5F4335D1

5F4335D2

5F4335D3

5F4335D4

5F4335D5

5F4335D6

5F4335D7

5F4335D8

5F4335D9

5F4335DA

5F4335DB

5F4335DC

5F4335DD

5F4335DE

5F4335DF

5F4335E0

5F4335E1

5F4335E2

5F4335E3

5F4335E4

5F4335E5

5F4335E6

5F4335E7

5F4335E8

5F4335E9

5F4335EA

5F4335EB

5F4335EC

5F4335ED

5F4335EE

5F4335EF

5F4335F0

5F4335F1

5F4335F2

5F4335F3

5F4335F4

5F4335F5

5F4335F6

5F4335F7

5F4335F8

5F4335F9

5F4335FA

5F4335FB

5F4335FC

5F4335FD

5F4335FE

5F4335FF

5F433600

5F433601

5F433602

5F433603

5F433604

5F433605

5F433606

5F433607

5F433608

5F433609

5F43360A

5F43360B

5F43360C

5F43360D

5F43360E

5F43360F

5F433610

5F433611

5F433612

5F433613

5F433614

5F433615

5F433616

5F433617

5F433618

5F433619

5F43361A

5F43361B

5F43361C

5F43361D

5F43361E

5F43361F

5F433620

5F433621

5F433622

5F433623

5F433624

5F433625

5F433626

5F433627

5F433628

5F433629

5F43362A

5F43362B

5F43362C

5F43362D

5F43362E

5F43362F

5F433630

5F433631

5F433632

5F433633

5F433634

5F433635

5F433636

5F433637

5F433638

5F433639

5F43363A

5F43363B

5F43363C

5F43363D

5F43363E

5F43363F

5F433640

5F433641

5F433642

5F433643

5F433644

5F433645

5F433646

5F433647

5F433648

5F433649

5F43364A

5F43364B

5F43364C

5F43364D

5F43364E

5F43364F

5F433650

5F433651

5F433652

5F433653

5F433654

5F433655

5F433656

5F433657

5F433658

5F433659

5F43365A

5F43365B

5F43365C

5F43365D

5F43365E

5F43365F

5F433660

5F433661

5F433662

5F433663

5F433664

5F433665

5F433666

5F433667

5F433668

5F433669

5F43366A

5F43366B

5F43366C

5F43366D

5F43366E

5F43366F

5F433670

5F433671

5F433672

5F433673

5F433674

5F433675

5F433676

5F433677

5F433678

5F433679

5F43367A

5F43367B

5F43367C

5F43367D

5F43367E

5F43367F

5F433680

5F433681

5F433682

5F433683

5F433684

5F433685

5F433686

5F433687

5F433688

5F433689

5F43368A

5F43368B

5F43368C

5F43368D

5F43368E

5F43368F

5F433690

5F433691

5F433692

5F433693

5F433694

5F433695

5F433696

5F433697

5F433698

5F433699

5F43369A

5F43369B

5F43369C

5F43369D

5F43369E

5F43369F

5F4336A0

5F4336A1

5F4336A2

5F4336A3

5F4336A4

5F4336A5

5F4336A6

5F4336A7

5F4336A8

5F4336A9

5F4336AA

5F4336AB

5F4336AC

5F4336AD

5F4336AE

5F4336AF

5F4336B0

5F4336B1

5F4336B2

5F4336B3

5F4336B4

5F4336B5

5F4336B6

5F4336B7

5F4336B8

5F4336B9

5F4336BA

5F4336BB

5F4336BC

5F4336BD

5F4336BE

5F4336BF

5F4336C0

5F4336C1

5F4336C2

5F4336C3

5F4336C4

5F4336C5

5F4336C6

5F4336C7

5F4336C8

5F4336C9

5F4336CA

5F4336CB

5F4336CC

5F4336CD

5F4336CE

5F4336CF

5F4336D0

5F4336D1

5F4336D2

5F4336D3

5F4336D4

5F4336D5

5F4336D6

5F4336D7

5F4336D8

5F4336D9

5F4336DA

5F4336DB

5F4336DC

5F4336DD

5F4336DE

5F4336DF

5F4336E0

5F4336E1

5F4336E2

5F4336E3

5F4336E4

5F4336E5

5F4336E6

5F4336E7

5F4336E8

5F4336E9

5F4336EA

5F4336EB

5F4336EC

5F4336ED

5F4336EE

5F4336EF

5F4336F0

5F4336F1

5F4336F2

5F4336F3

5F4336F4

5F4336F5

5F4336F6

5F4336F7

5F4336F8

5F4336F9

5F4336FA

5F4336FB

5F4336FC

5F4336FD

5F4336FE

5F4336FF

5F433700

5F433701

5F433702

5F433703

5F433704

5F433705

5F433706

5F433707

5F433708

5F433709

5F43370A

5F43370B

5F43370C

5F43370D

5F43370E

5F43370F

5F433710

5F433711

5F433712

5F433713

5F433714

5F433715

5F433716

5F433717

5F433718

5F433719

5F43371A

5F43371B

5F43371C

5F43371D

5F43371E

5F43371F

5F433720

5F433721

5F433722

5F433723

5F433724

5F433725

5F433726

5F433727

5F433728

5F433729

5F43372A

5F43372B

5F43372C

5F43372D

5F43372E

5F43372F

5F433730

5F433731

5F433732

5F433733

5F433734

5F433735

5F433736

5F433737

5F433738

5F433739

5F43373A

5F43373B

5F43373C

5F43373D

5F43373E

5F43373F

5F433740

5F433741

5F433742

5F433743

5F433744

5F433745

5F433746

5F433747

5F433748

5F433749

5F43374A

5F43374B

5F43374C

5F43374D

5F43374E

5F43374F

5F433750

5F433751

5F433752

5F433753

5F433754

5F433755

5F433756

5F433757

5F433758

5F433759

5F43375A

5F43375B

5F43375C

5F43375D

5F43375E

5F43375F

5F433760

5F433761

5F433762

5F433763

5F433764

5F433765

5F433766

5F433767

5F433768

5F433769

5F43376A

5F43376B

5F43376C

5F43376D

5F43376E

5F43376F

5F433770

5F433771

5F433772

5F433773

5F433774

5F433775

5F433776

5F433777

5F433778

5F433779

5F43377A

5F43377B

5F43377C

5F43377D

5F43377E

5F43377F

5F433780

5F433781

5F433782

5F433783

5F433784

5F433785

5F433786

5F433787

5F433788

5F433789

5F43378A

5F43378B

5F43378C

5F43378D

5F43378E

5F43378F

5F433790

5F433791

5F433792

5F433793

5F433794

5F433795

5F433796

5F433797

5F433798

5F433799

5F43379A

5F43379B

5F43379C

5F43379D

5F43379E

5F43379F

5F4337A0

5F4337A1

5F4337A2

5F4337A3

5F4337A4

5F4337A5

5F4337A6

5F4337A7

5F4337A8

5F4337A9

5F4337AA

5F4337AB

5F4337AC

5F4337AD

5F4337AE

5F4337AF

5F4337B0

5F4337B1

5F4337B2

5F4337B3

5F4337B4

5F4337B5

5F4337B6

5F4337B7

5F4337B8

5F4337B9

5F4337BA

5F4337BB

5F4337BC

5F4337BD

5F4337BE

5F4337BF

5F4337C0

5F4337C1

5F4337C2

5F4337C3

5F4337C4

5F4337C5

5F4337C6

5F4337C7

5F4337C8

5F4337C9

5F4337CA

5F4337CB

5F4337CC

5F4337CD

5F4337CE

5F4337CF

5F4337D0

5F4337D1

5F4337D2

5F4337D3

5F4337D4

5F4337D5

5F4337D6

5F4337D7

5F4337D8

5F4337D9

5F4337DA

5F4337DB

5F4337DC

5F4337DD

5F4337DE

5F4337DF

5F4337E0

5F4337E1

5F4337E2

5F4337E3

5F4337E4

5F4337E5

5F4337E6

5F4337E7

5F4337E8

5F4337E9

5F4337EA

5F4337EB

5F4337EC

5F4337ED

5F4337EE

5F4337EF

5F4337F0

5F4337F1

5F4337F2

5F4337F3

5F4337F4

5F4337F5

5F4337F6

5F4337F7

5F4337F8

5F4337F9

5F4337FA

5F4337FB

5F4337FC

5F4337FD

5F4337FE

5F4337FF

5F433800

5F433801

5F433802

5F433803

5F433804

5F433805

5F433806

5F433807

5F433808

5F433809

5F43380A

5F43380B

5F43380C

5F43380D

5F43380E

5F43380F

5F433810

5F433811

5F433812

5F433813

5F433814

5F433815

5F433816

5F433817

5F433818

5F433819

5F43381A

5F43381B

5F43381C

5F43381D

5F43381E

5F43381F

5F433820

5F433821

5F433822

5F433823

5F433824

5F433825

5F433826

5F433827

5F433828

5F433829

5F43382A

5F43382B

5F43382C

5F43382D

5F43382E

5F43382F

5F433830

5F433831

5F433832

5F433833

5F433834

5F433835

5F433836

5F433837

5F433838

5F433839

5F43383A

5F43383B

5F43383C

5F43383D

5F43383E

5F43383F

5F43384

PROOVE THAT EVERY TOOL
CAN BETRUSTED

PEOPLE AND PROCESSES

“Insisting that operators always follow procedures does not guarantee safety although it does usually guarantee that there is someone to blame-either for following the procedures or for not following them-when things go wrong.”

NANCY LEVESON



ROOT CAUSE ANALYSIS



Why?



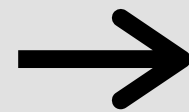
ROOT CAUSE ANALYSIS



Root
cause



?

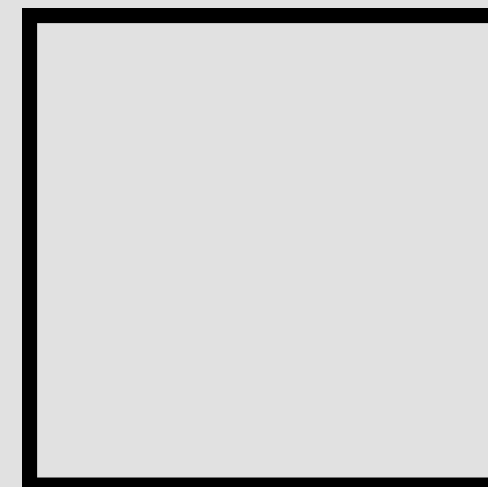
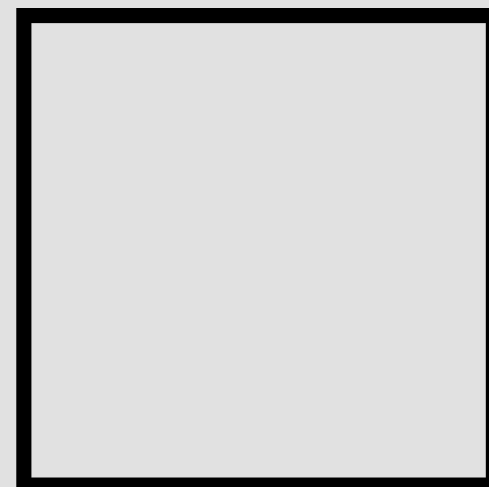


Accident

ROOT CAUSE ANALYSIS



Root
cause



Accident

ROOT CAUSE ANALYSIS



?

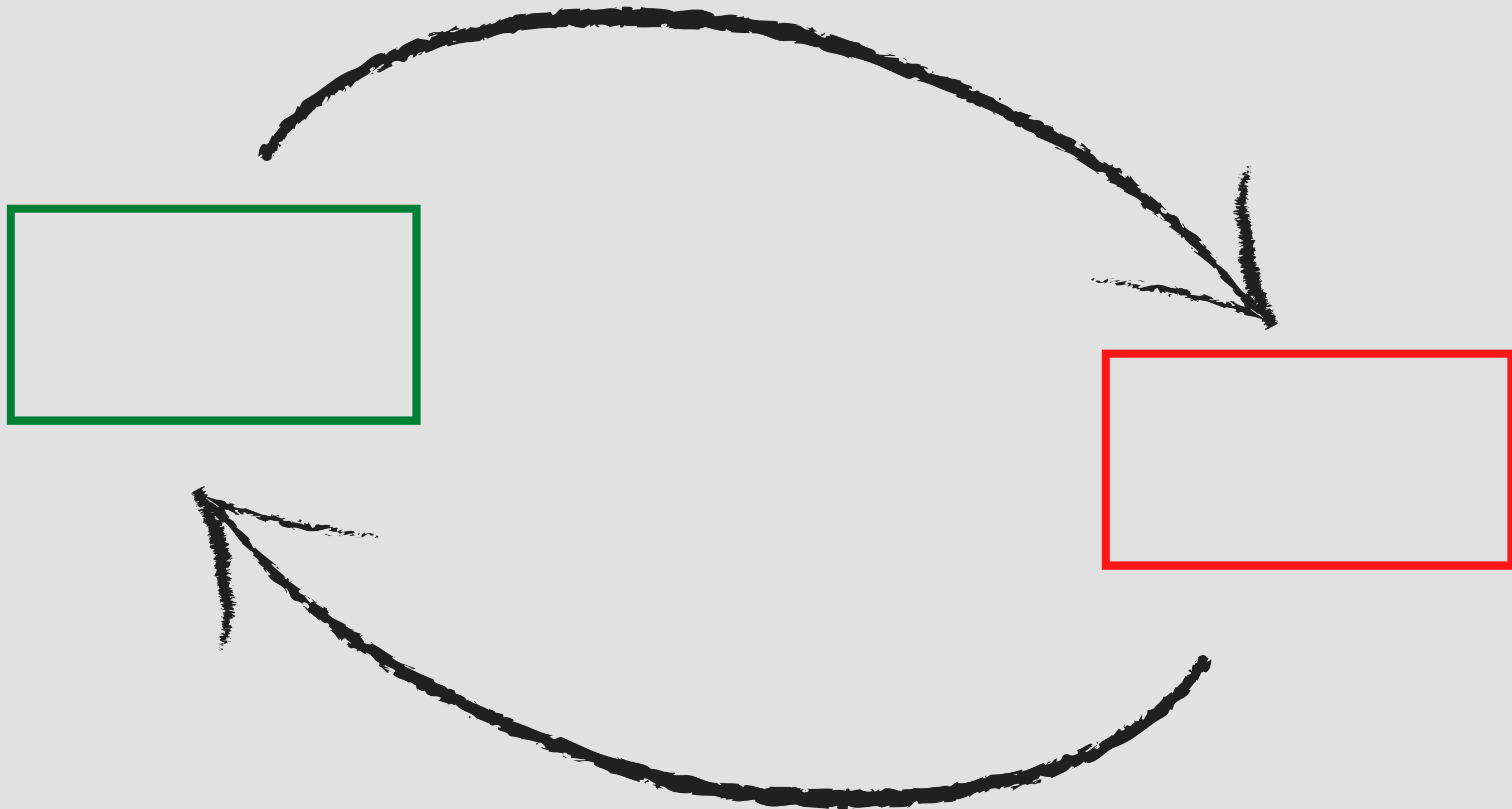


Root
cause



Accident

FEEDBACK LOOP



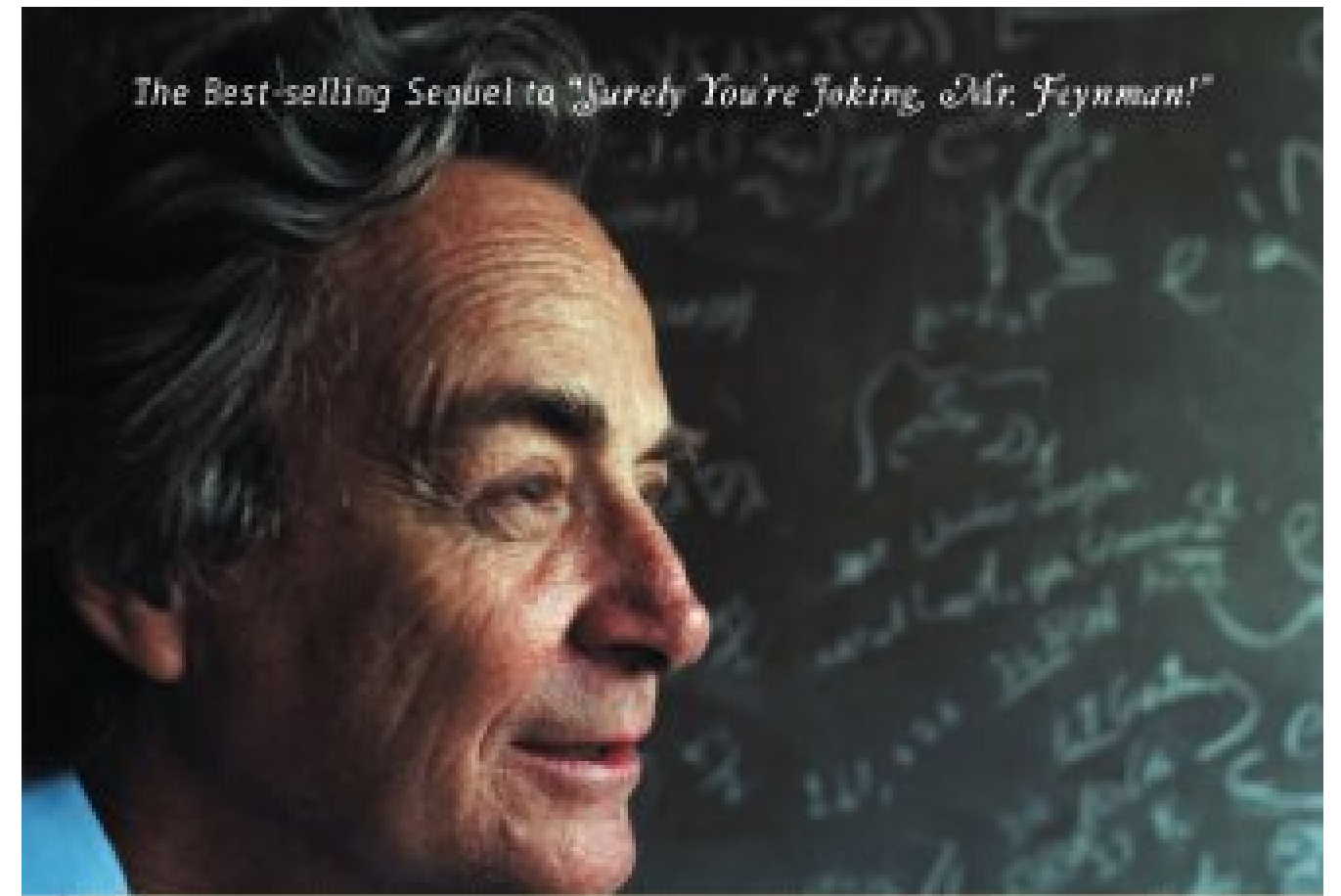
Engineering a Safer World

Systems Thinking Applied
to Safety

Nancy G. Leveson



The Best-selling Sequel to "Surely You're Joking, Mr. Feynman!"



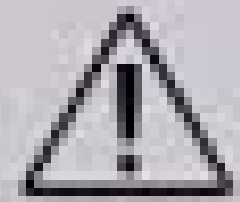
*"What Do **You** Care
What Other People Think?"*

*Further Adventures
of a Curious Character*

RICHARD P. FEYNMAN







EMERGENCY ALERTS

now

Emergency Alert

BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

Slide for more



NIGHTLY
 NEWS

Location: **HELM**

Steering Mode: **COMPUTER MANUAL**

☐ HDG Monitor

☐ RRS

2B Port Pumps 2A

NO FAULT

NO FAULT

LCU NORMAL

LCU NORMAL

HPU NORMAL

HPU NORMAL

☐ Stop

☐ Stop

☐ Run

☐ Run

☐ Engage

☐ Engage

1B Stbd Pumps 1A

NO FAULT

NO FAULT

LCU NORMAL

LCU NORMAL

HPU NORMAL

HPU NORMAL

☐ Stop

☐ Stop

☐ Run

☐ Run

☐ Engage

☐ Engage



Port

Control Location

Thrust **HELM**

Aux **UCC3** EOT

RPM **87** Brake Pitch % **100**

RPM **87** Actual **100**

RPM **87** Order **100**

RPM **87** Acknowledge **100**

PCL **2513**

Accept

Cancel

Mode Select

☒ Gang

All Stop

☒ Alarm Ack.

☐ Bell Log Print

Whistle Control

Nixie Secured

Starboard

Control Location

Thrust **HELM**

Aux **UCC3** EOT

RPM **87** Brake Pitch % **100**

RPM **87** Actual **100**

RPM **87** Order **100**

RPM **87** Acknowledge **100**

PCL **2513**

Accept

Cancel

Flank

Ahead Full

Std

Ahead 2/3

Ahead 1/3

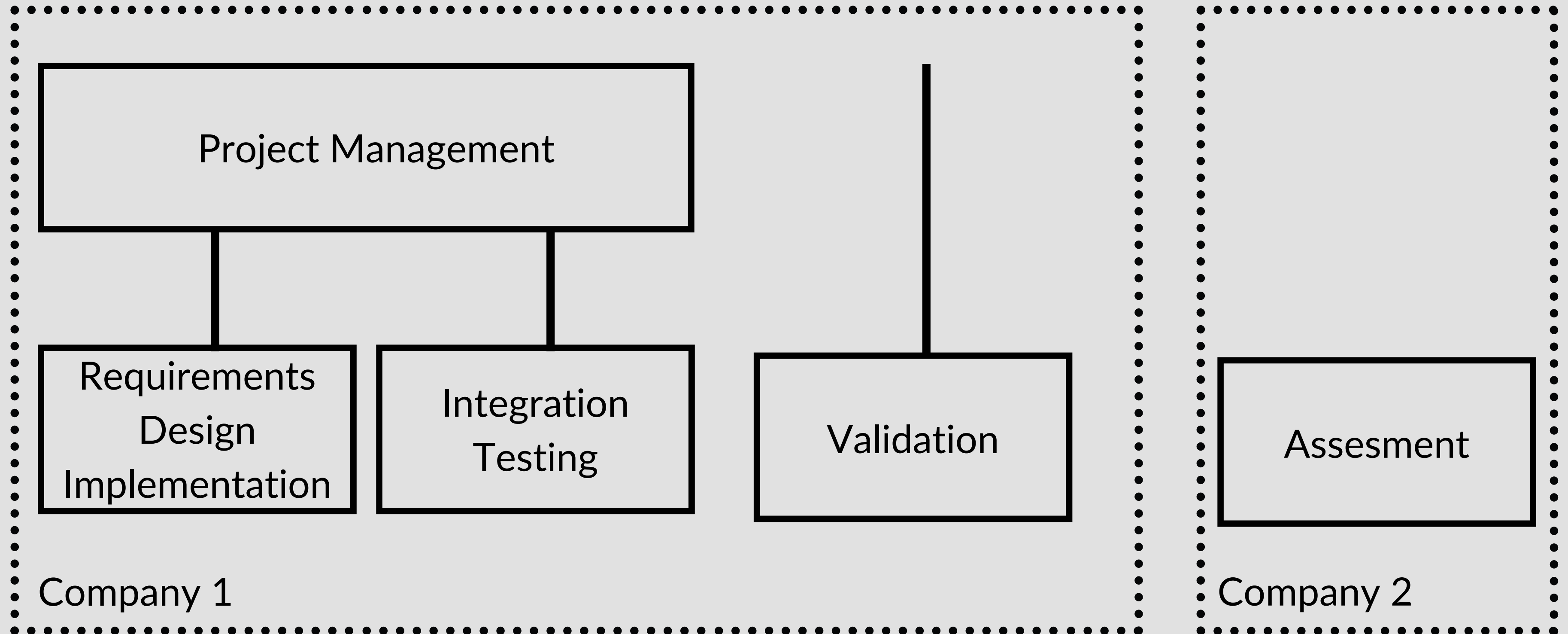
Stop

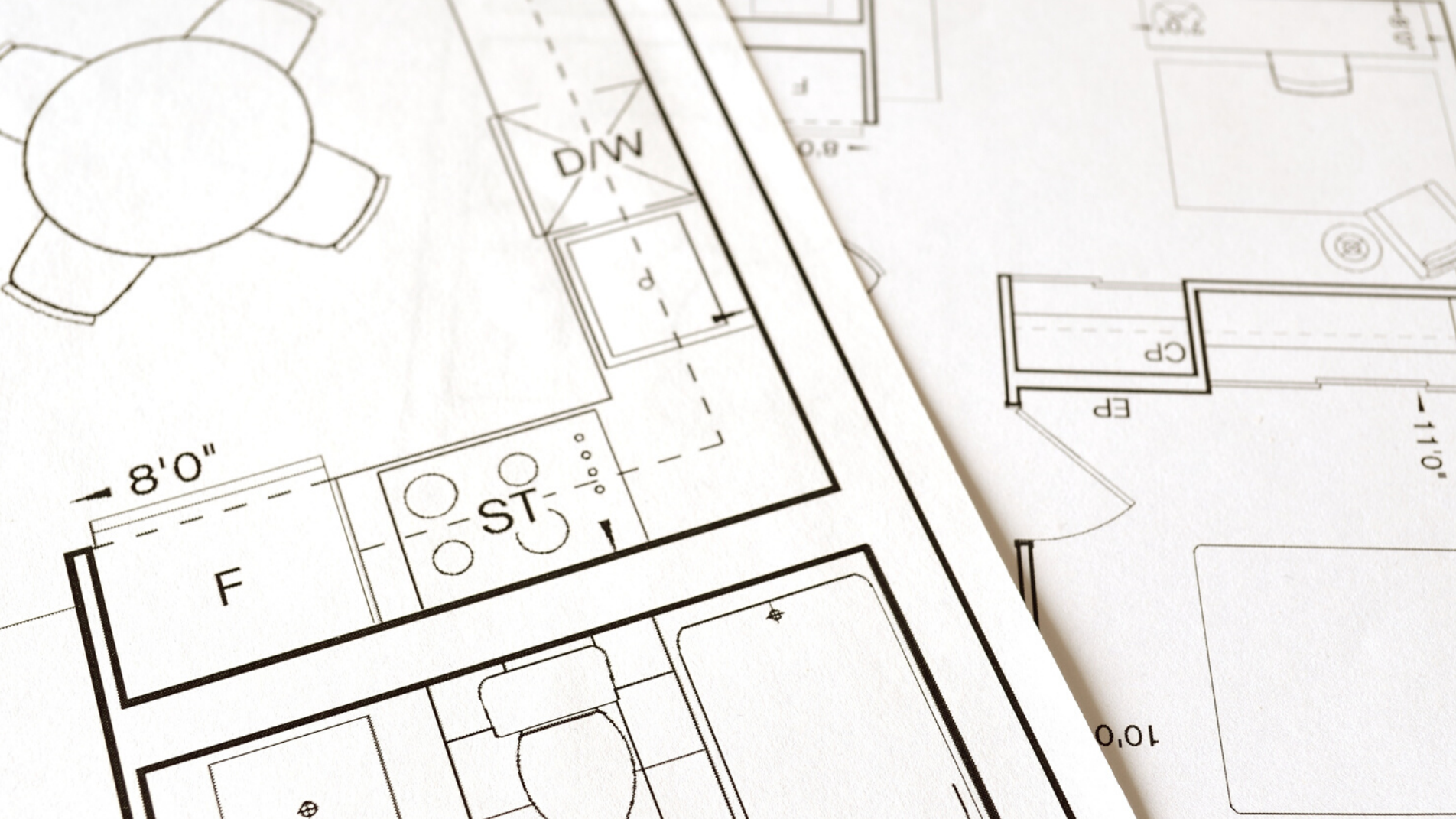
Back 1/3

Back 2/3

Back Full

PROJECT ROLES - SIL4





THANK YOU

<https://ucgosu.pl/slides-ndc-oslo-2020>

<https://solwit.com>

<https://ucgosu.pl>

Twitter: @MaciekGajdzica

Icons from:

<https://www.flaticon.com/>





ADDITIONAL RESOURCES

Boeing accident preliminary report:

<https://transportation.house.gov/imo/media/doc/TI%20Preliminary%20Investigative%20Findings%20Boeing%20737%20MAX%20March%202020.pdf>

Ship crash near Singapore analysis:

<https://features.propublica.org/navy-uss-mccain-crash/navy-installed-touch-screen-steering-ten-sailors-paid-with-their-lives/>

Hawaii false nuclear alert:

https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert