EUROPEAN CENTRAL BANK

TARGET2
- Abnormal situations -

Common presentation for the use at national level with the respective TARGET2 user community

Updated version 5 July 2007

I Placement in the framework

I Placement in the framework

Status

- Eurosystem achieved with TWG clarity on framework for abnormal situations. Discussions covered a situation that might last until the next calendar day.
- Need to make framework *transparent* to T2 users by a common presentation. This presentation has been updated (see yellow circles in the right top corner).
- A national dialogue with users on abnormal situations was held in Jan/Feb 2007. Such dialogue is considered to be a continuous exercise.

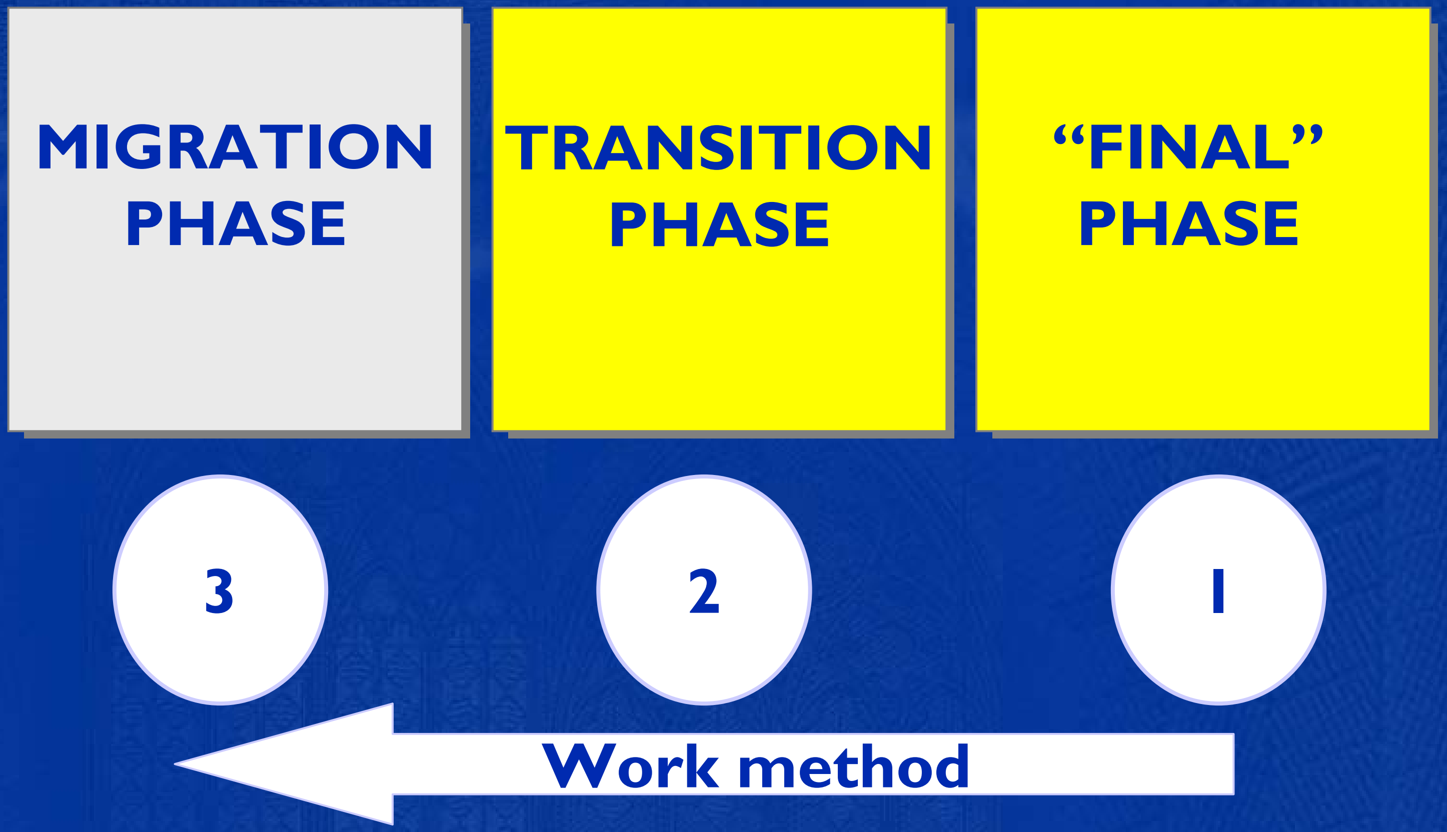
What is an abnormal situation (incident)?

- A situation preventing T2 from functioning normally and that (might) cause an interruption or reduction in the quality of service.
- Incident may derive from:
  - ❑ A failure of a relevant component or software in the system’s technical platform
  - ❑ A procedural, operational or business failure
  - ❑ A strike or major external event (natural disaster, power outage, terrorist attacks)

2 Followed approach

2 Followed approach

Three phases of TARGET2



MIGRATION PHASE

TRANSITION PHASE

"FINAL" PHASE

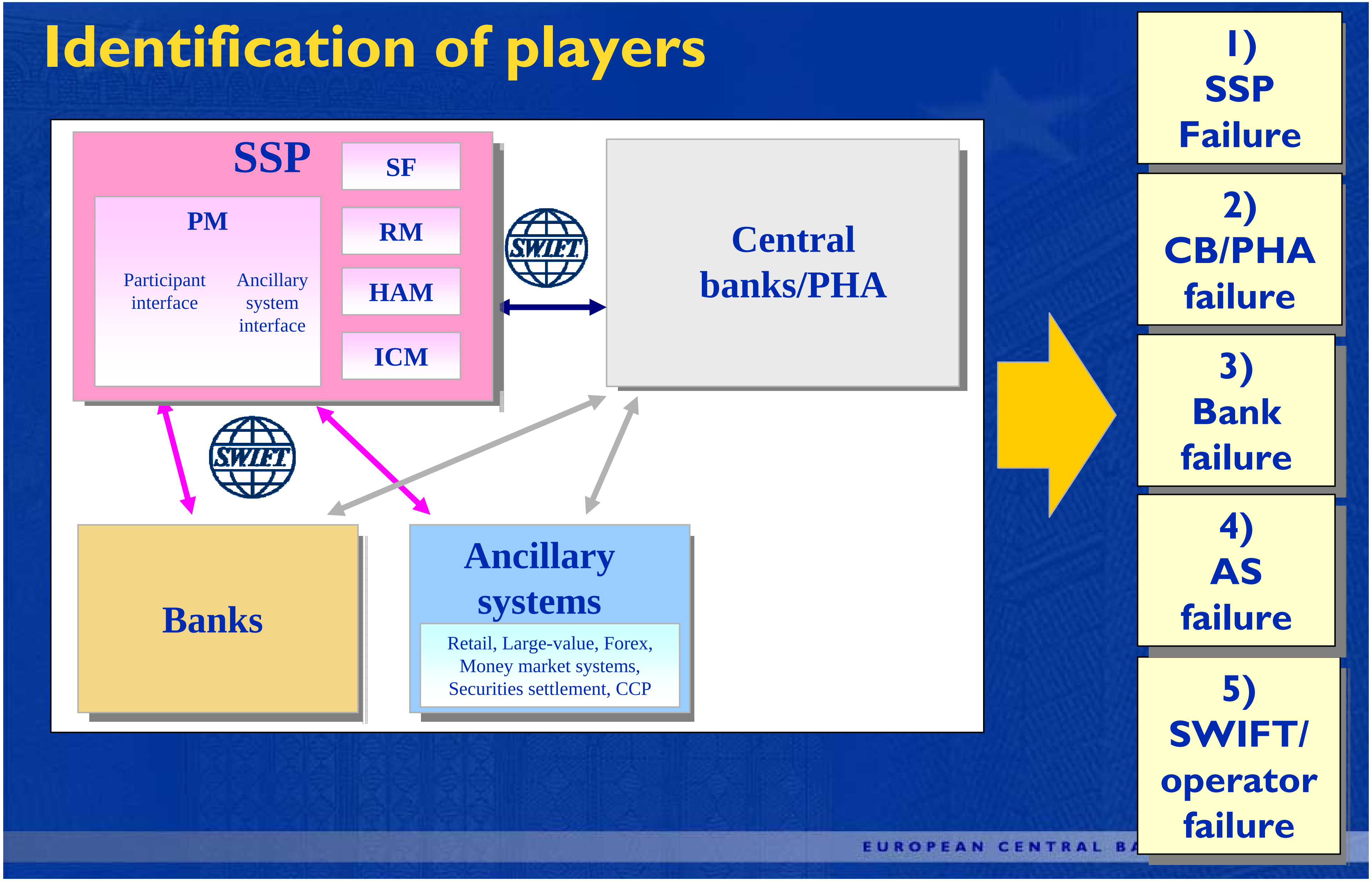
3

2

1

Work method

2 Followed approach



Identification of players

SSP

PM

Participant interface

Ancillary system interface

SF

RM

HAM

ICM

SWIFT

Central banks/PHA

SWIFT

Banks

Ancillary systems

Retail, Large-value, Forex, Money market systems, Securities settlement, CCP

1) SSP Failure

2) CB/PHA failure

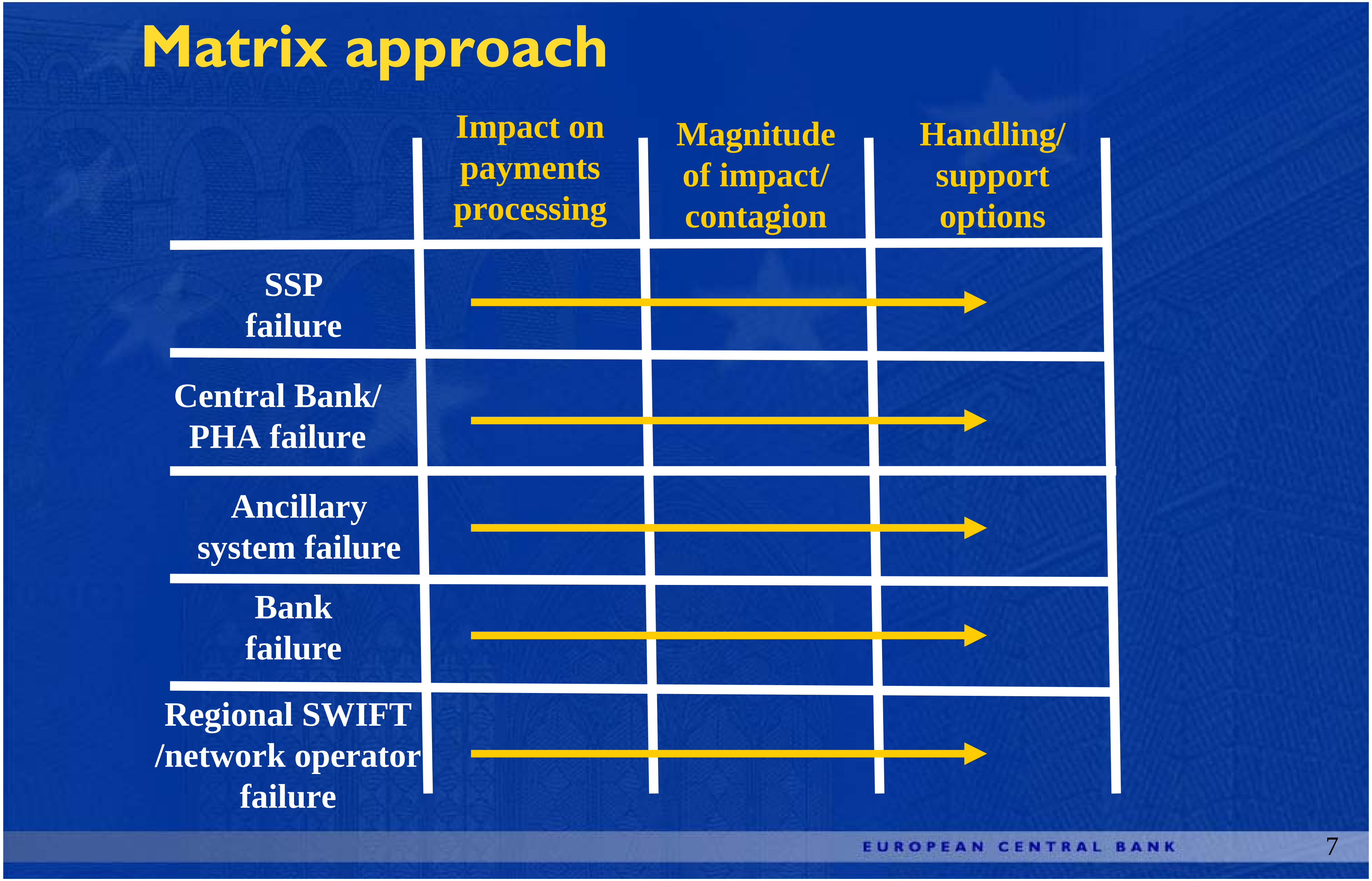
3) Bank failure

4) AS failure

5) SWIFT/ operator failure

EUROPEAN CENTRAL BA

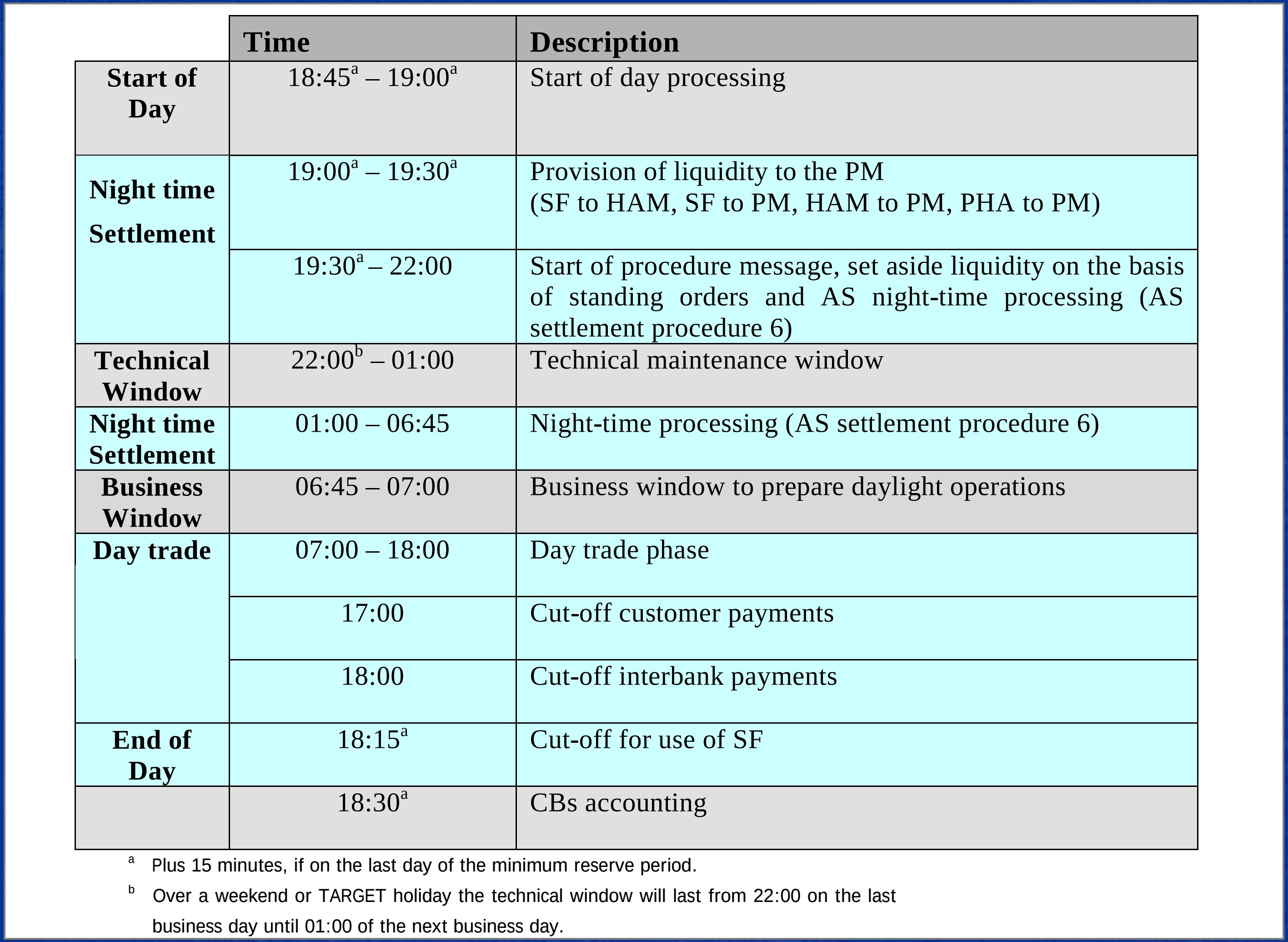
2 Followed approach



Matrix approach

	Impact on payments processing	Magnitude of impact/ contagion	Handling/ support options
SSP failure	→	→	→
Central Bank/ PHA failure	→	→	→
Ancillary system failure	→	→	→
Bank failure	→	→	→
Regional SWIFT /network operator failure	→	→	→

Entire T2 operational day covered

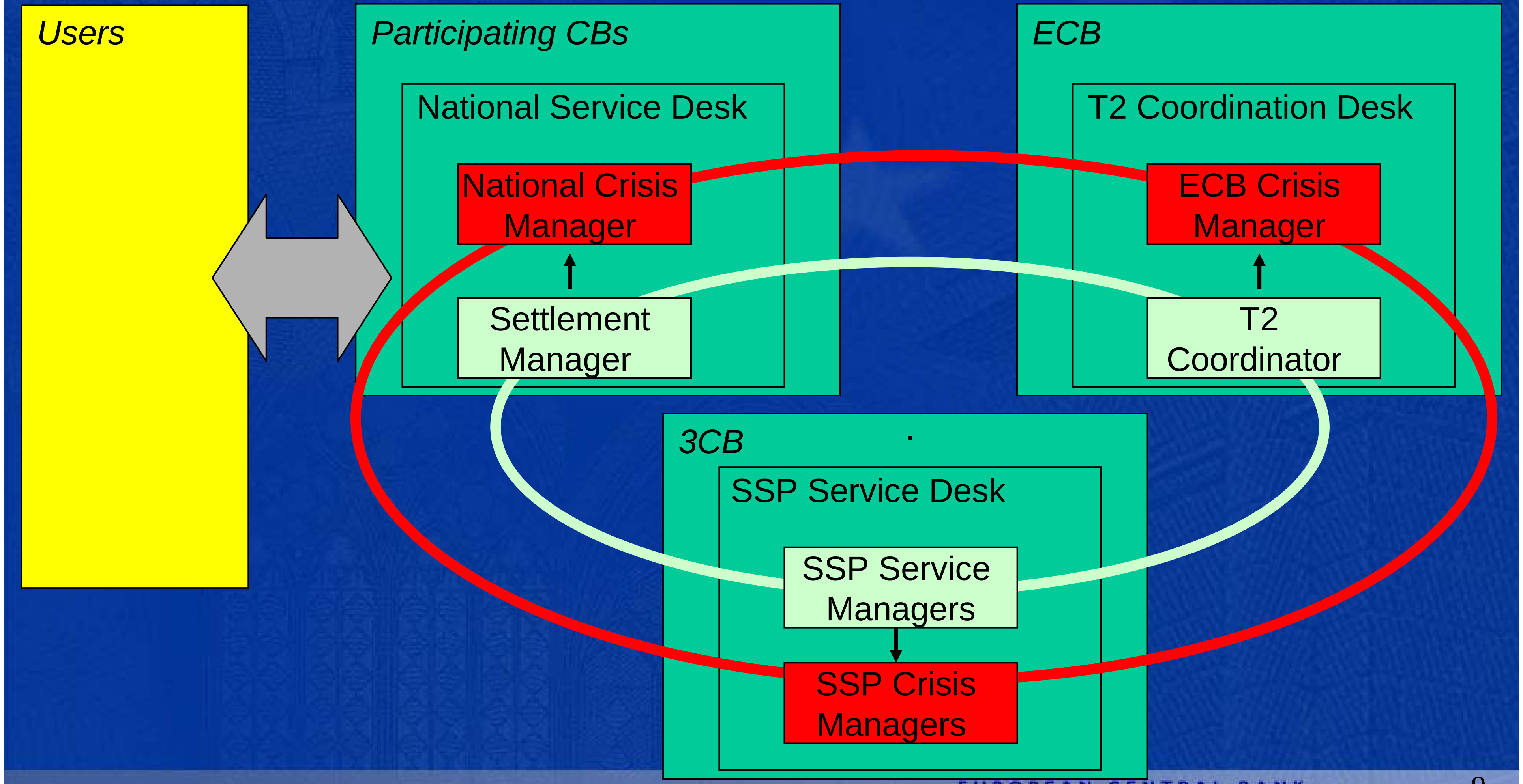


	Time	Description
Start of Day	18:45[a] – 19:00[a]	Start of day processing
Night time Settlement	19:00[a] – 19:30[a]	Provision of liquidity to the PM (SF to HAM, SF to PM, HAM to PM, PHA to PM)
	19:30[a] – 22:00	Start of procedure message, set aside liquidity on the basis of standing orders and AS night-time processing (AS settlement procedure 6)
Technical Window	22:00[b] – 01:00	Technical maintenance window
Night time Settlement	01:00 – 06:45	Night-time processing (AS settlement procedure 6)
Business Window	06:45 – 07:00	Business window to prepare daylight operations
Day trade	07:00 – 18:00	Day trade phase
	17:00	Cut-off customer payments
	18:00	Cut-off interbank payments
End of Day	18:15[a]	Cut-off for use of SF
	18:30[a]	CBs accounting

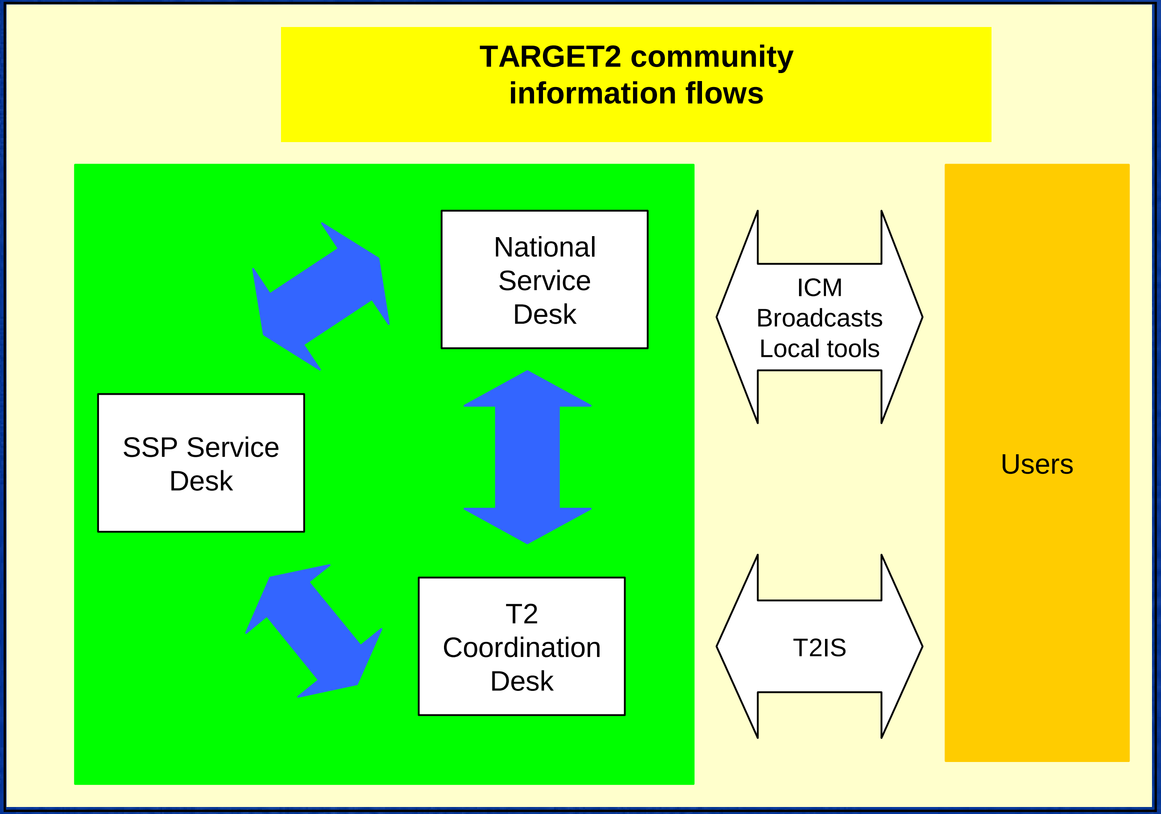
[a] Plus 15 minutes, if on the last day of the minimum reserve period.

[b] Over a weekend or TARGET holiday the technical window will last from 22:00 on the last business day until 01:00 of the next business day.

Business relationship



Communication relationship



3 SSP Failure

Importance

- SSP failure comes along with potential systemic risk
  - Stop of processing of TARGET2 payments
  - Blockage of liquidity (payments capacity in the SSP)
  - Potential impacts on users, other market infrastructures, and markets
  - Potential impacts across countries and currencies

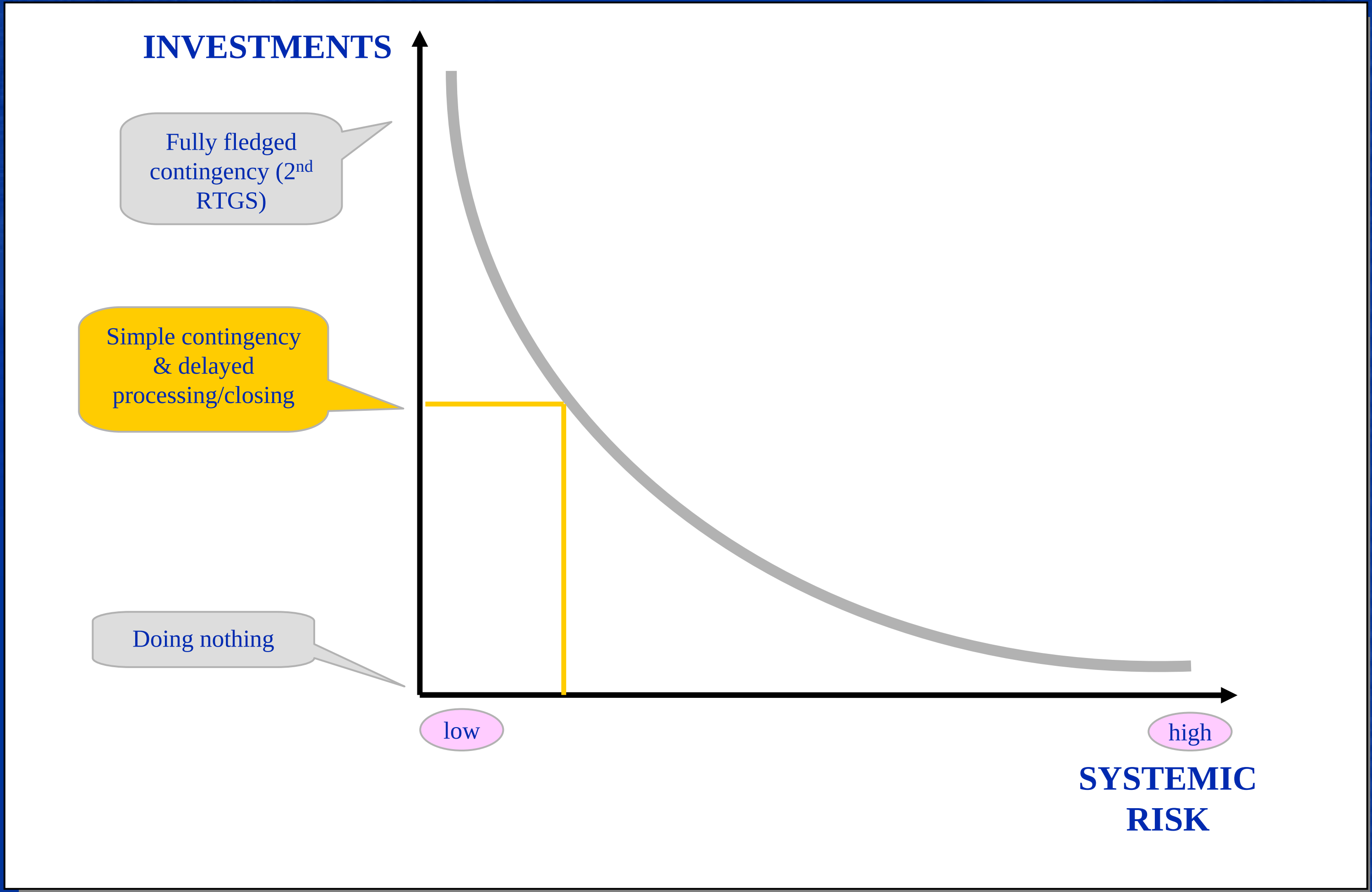
3 SSP failure

Principles

- First, try to fix the problem.
- Business continuity, i.e. restoration of full business by failing over form a primary site/region to a back-up site/region, emphasised.
- Contingency means running limited business operations. Systemically important payments are processed in contingency, while the remainder payments are delayed in processing until SSP recovery.
- T2 delayed closing gives additional operational time for problem fixing/business continuity.
- PHAs keep on processing during a SSP failure.

3 SSP failure

Striking the balance


INVESTMENTS
Fully fledged contingency (2nd RTGS)
Simple contingency & delayed processing/closing
Doing nothing
low
high
SYSTEMIC RISK

3 SSP Failure

- Business Continuity -

3 SSP failure – Business Continuity

Principles

Business continuity means switching from a primary site/region to a back-up site/region.

Events:

- Smaller failures covered by redundancy of main critical elements within same site.
- Major failures or disasters (e.g. fire, flood, terrorist attack, IT fault, telecommunications fault) call for business continuity, i.e. switching form a primary site/region to a back up site/region.

3 SSP failure – Business Continuity

Principles

Business continuity embraces intra-region failover and inter-region failover.

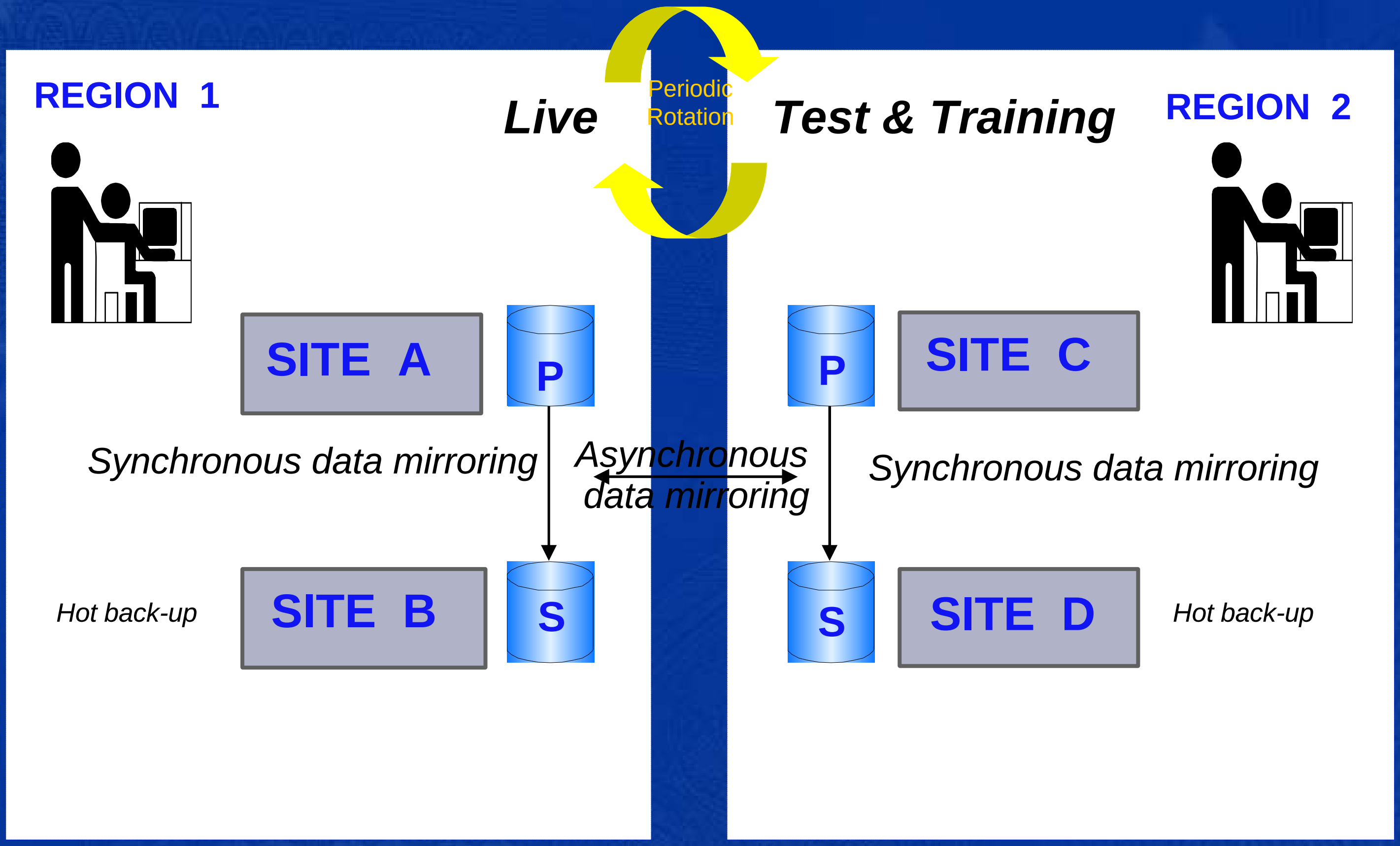
Type of SSP failure determines decision to failover. No sequential order of intra-region failover and inter-region failover.

In case of a SSP failure, the decision is made either to conduct an intra-region failover or an inter-region failover.

Inter-region failover activated in case of very exceptional circumstances (very low likelihood).

Fail-over scheme applied throughout T2 operational day.

3 SSP failure – Business Continuity



REGION 1

Live

Periodic Rotation

Test & Training

REGION 2

SITE A

P

Synchronous data mirroring

Asynchronous data mirroring

P

SITE C

Synchronous data mirroring

Hot back-up

SITE B

S

S

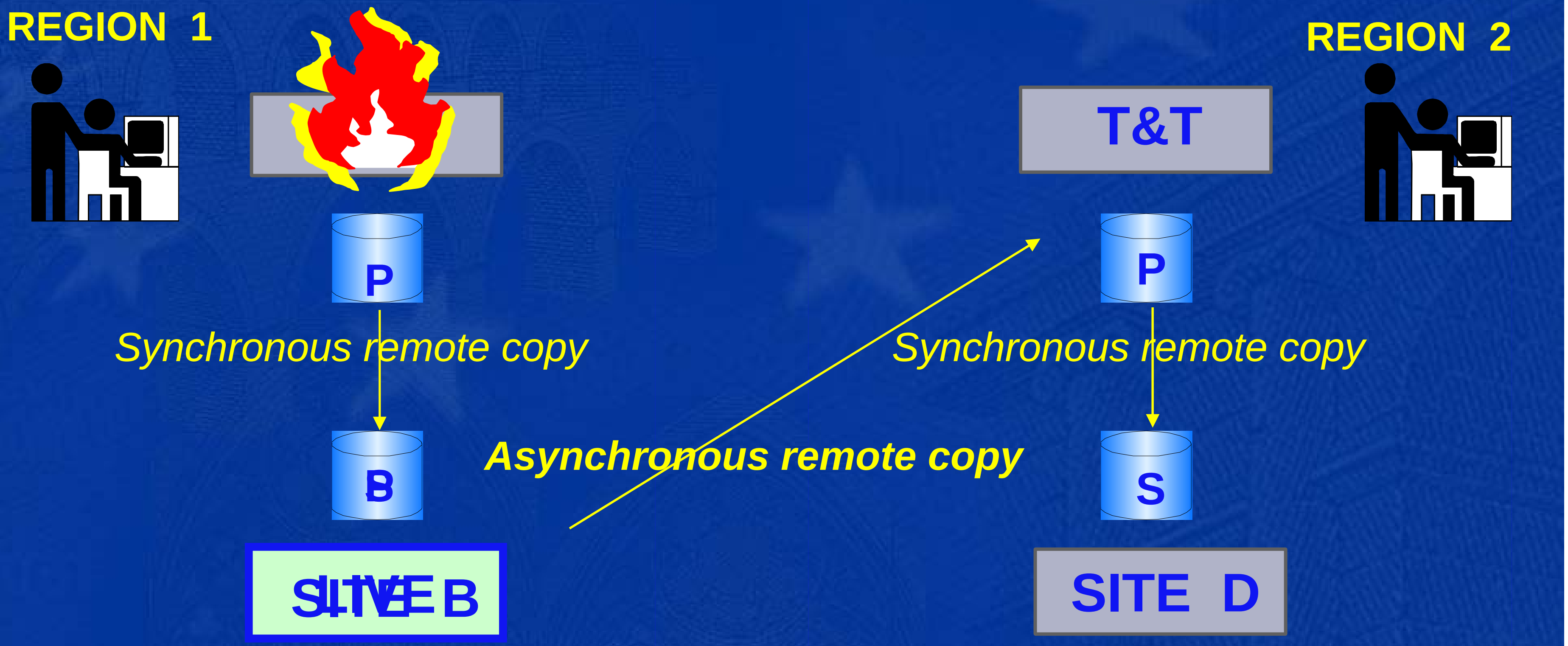
SITE D

Hot back-up

Intra-regional recovery can last at the most 1 hour (without taking into account decision-making time) with no loss of data updates.

the secondary region has to re-start within two hours (without considering the decision-making time the duration of which will be defined at a later stage)

Intra-region failover



REGION 1

REGION 2

T&T

P

P

Synchronous remote copy

Synchronous remote copy

B

S

Asynchronous remote copy

LIVE

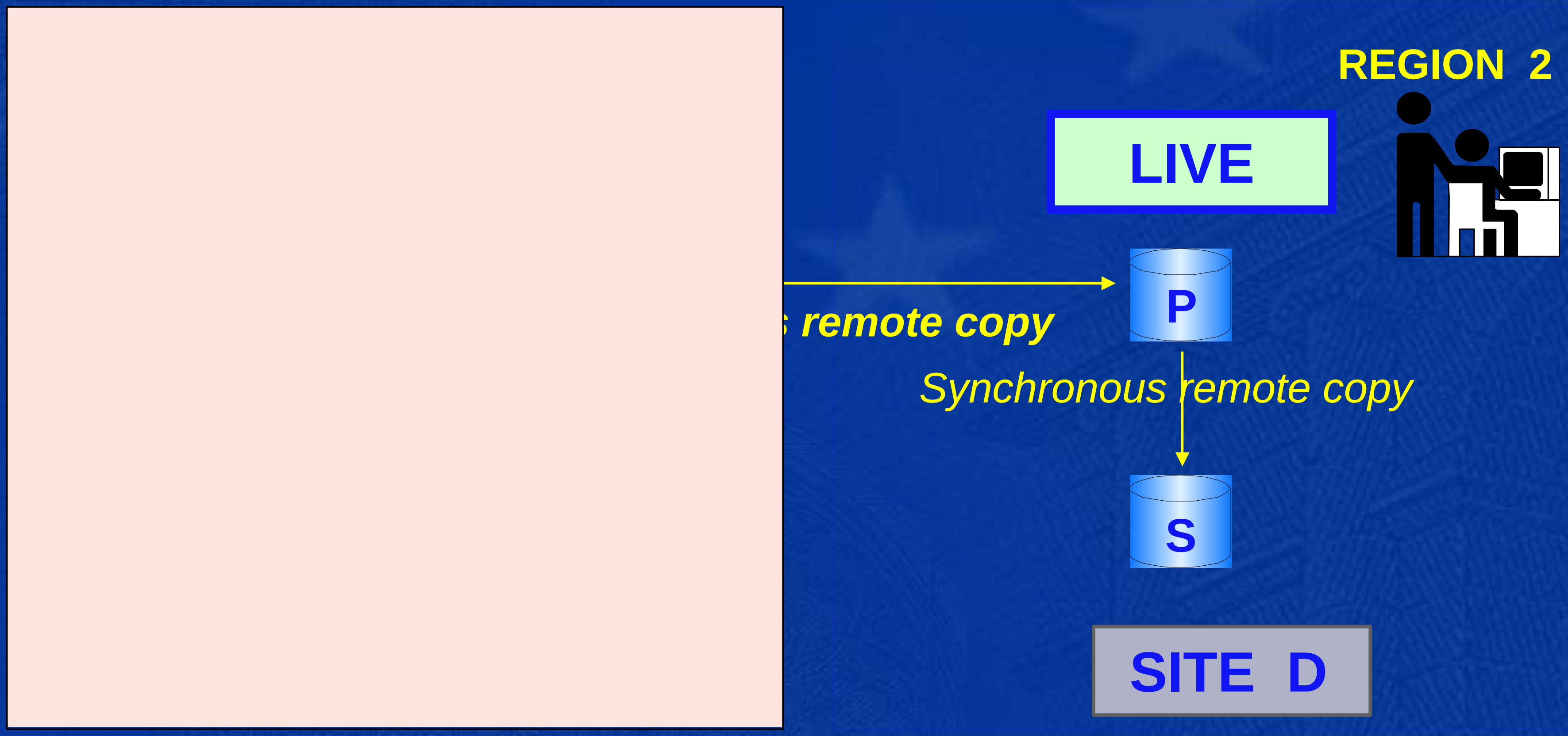
SITE B

SITE D

Intra-region failover

- Failing over from site A to site B within the same region
- Synchronous copying
  - Databases are exactly the same
  - No reconciliation necessary
- Continuation 1 hour max. after decision
- Users can keep on sending SWIFT Net FIN payments as well as FileAct (in store and forward mode)

Inter-region failover



3 SSP failure – Business Continuity

Inter-region failover

- Failing over from Region 1 to Region 2
- Geographical distance requires asynchronous copying
  - Databases are showing a time gap of max. 2 min
  - Reconciliation only necessary in rare situations (see next slide)
- Continuation 2 hours max. after decision
- Users can keep on sending SWIFT Net FIN payments but should stop sending FileAct (in store and forward mode)

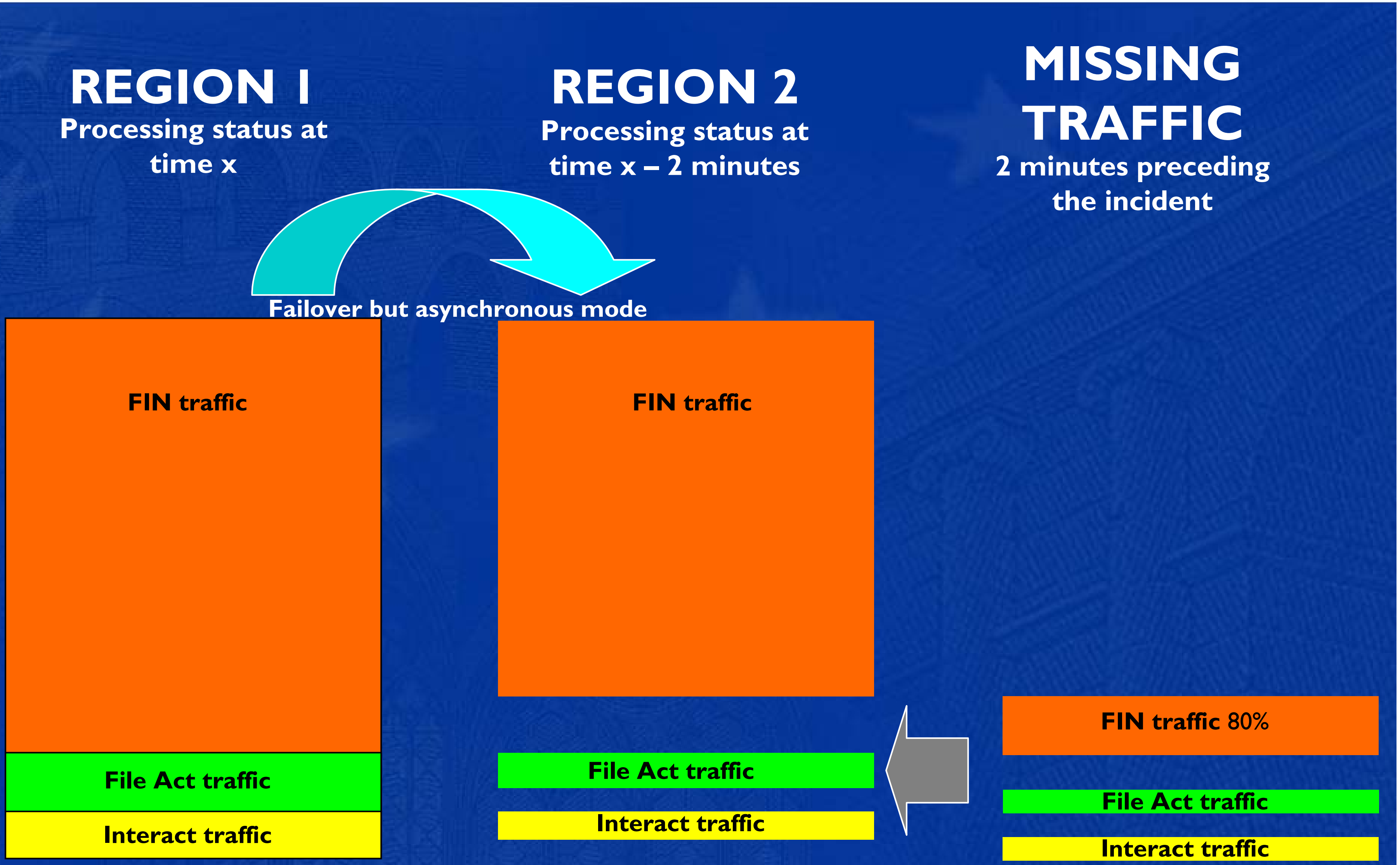
3 SSP failure – Business Continuity

Inter-region failover

An inter-region failover with a loss of data can only occur in the event that both sites in the active region would fail simultaneously (very low liklihood).

Only in such scenario will a rebuilding procedure be required with the involvement of the T2 users!

3 SSP failure – Business Continuity



REGION 1

Processing status at time x

REGION 2

Processing status at time x – 2 minutes

MISSING TRAFFIC

2 minutes preceding the incident

Failover but asynchronous mode

FIN traffic

File Act traffic

Interact traffic

FIN traffic

File Act traffic

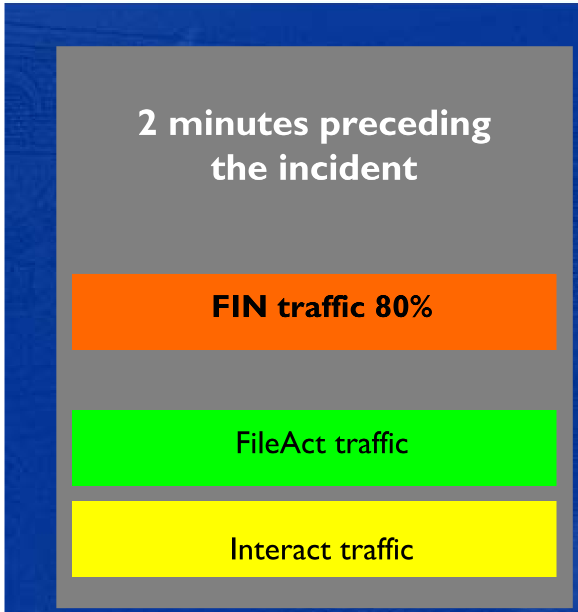
Interact traffic

FIN traffic 80%

File Act traffic

Interact traffic

3 SSP failure – Business Continuity



2 minutes preceding the incident

FIN traffic 80%

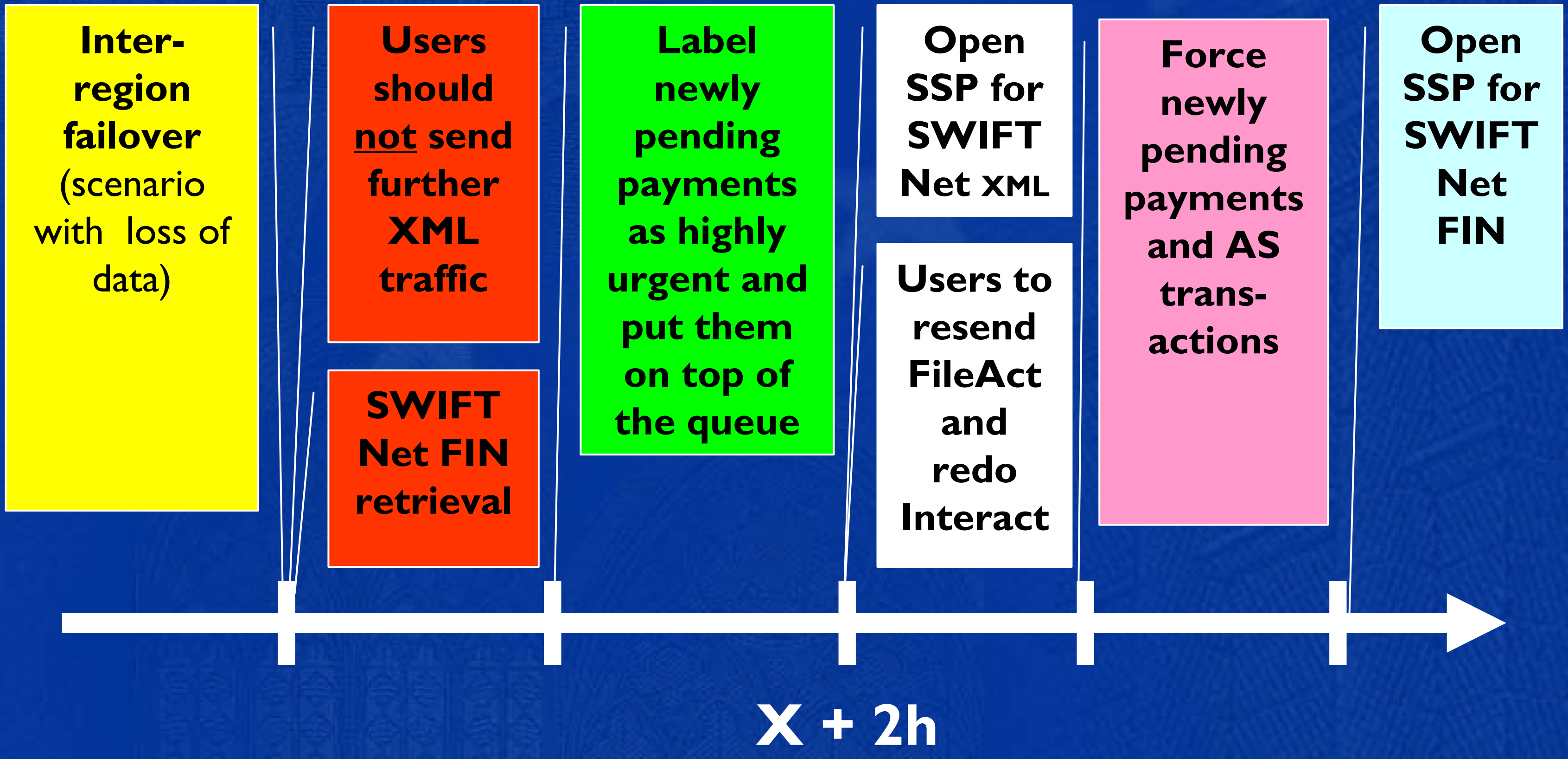
FileAct traffic

Interact traffic

- SWIFT retrieval of FIN messages and reconciliation
- No SWIFT retrieval function for Interact and FileAct
- Initial senders need to be involved

If not all XML traffic would be rebuilt, some payments/AS transactions reported as final in Region 1 could become “newly pending” in Region 2.

3 SSP failure – Business Continuity



Inter-region failover (scenario with loss of data)

Users should not send further XML traffic

SWIFT Net FIN retrieval

Label newly pending payments as highly urgent and put them on top of the queue

Open SSP for SWIFT Net XML

Users to resend FileAct and redo Interact

Force newly pending payments and AS trans-actions

Open SSP for SWIFT Net FIN

X + 2h

3 SSP failure – Business Continuity

- Step 1 and 2 (red boxes)
  - All users asked not to send any XML messages during failover.
  - The retrieval and reconciliation of SWIFTNet FIN messages takes place:
    - Based on sent MT 096 and received MT 097
    - Matching couples will be booked in Region 2
    - MT 096 without MT 097 will be queued (possibly due to missing /FileAct/InterAct messages) ➔ these payments will be shown as pending

3 SSP failure – Business Continuity

- Step 3 (green box)
  - These payments are shown in the ICM as:
    - „newly pending payments“ and
    - would be labelled as highly urgent and
    - put on the top of the queue

3 SSP failure – Business Continuity

- Step 4 and 5 (white boxes)
  - The SSP would be opened for SWIFTNet XML:
    - Users will get access to SSP data and can reconcile the processing status and check the list of pending payments
    - The AS are asked to resend any FileAct messages with the same reference they have sent 10 minutes before the incident or send those messages that they have identified as missing
    - ASs, CBs, Banks required to redo all their InterAct traffic they did 2 minutes before the incident
    - New XML traffic should not be sent

3 SSP failure – Business Continuity

- Step 6 (pink box)
  - Resent XML traffic will reduce “newly pending” payments.
  - If not all XML traffic would be resent or if any new XML traffic would have entered the system (e.g. against the recommendation, an AS has sent FileAct files that were stored at SWIFT level and flow in at the momemt TARGET2 was opened for SWIFT Net XML traffic) some payments and AS transactions might remain “newly pending”.
  - The respective NCB would force these “newly pending” payments and transactions.

3 SSP failure – Business Continuity

- Step 7 (blue box)
  - The SSP will be opened for SWIFTNet FIN and normal processing will start.
  - In case the CM was used, the balances of the CM will be transferred from the CM to the PM.

3 SSP failure – Business Continuity

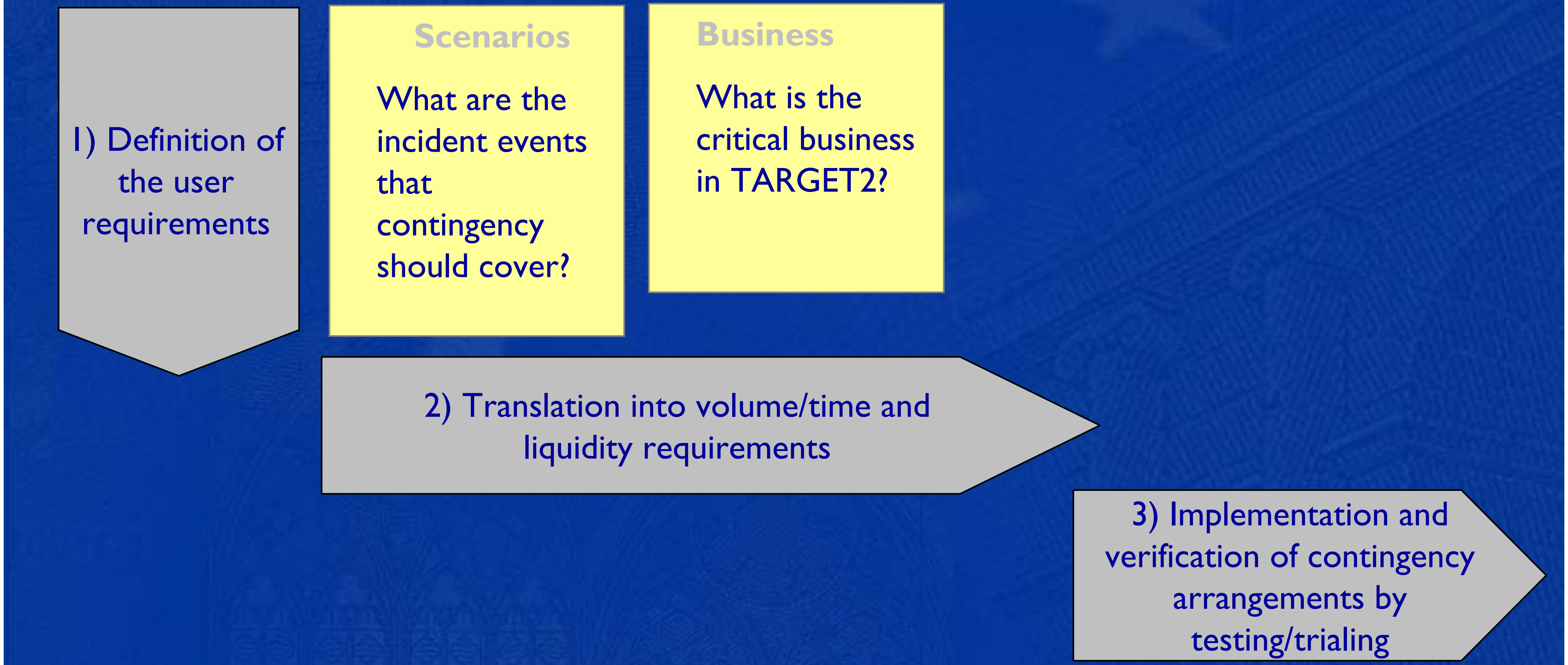
- Execution times (with rebuilding process)
  - Payments with code word /REJTIME/ will not be rejected

- Optional mechanisms (with rebuilding process)
  - The information period will be set to 15 minutes before „cut-off customer“.
  - Settlement period will be set to „cut-off customer“.

3 SSP Failure

- Contingency -

Approach taken for TARGET2 contingency



1) Definition of the user requirements

Scenarios

What are the incident events that contingency should cover?

Business

What is the critical business in TARGET2?

2) Translation into volume/time and liquidity requirements

3) Implementation and verification of contingency arrangements by testing/trialing

3 SSP failure - Contingency

Principles

- TARGET2 payments are processed in real-time and it guarantees the “same day processing” in case of abnormal situations

- Some very critical payments cannot wait for recovery and are delayed in processing until SSP recovery require immediate processing, while other euro-area “clean” TARGET2 payments

3 SSP failure - Contingency

Principles

Contingency processing via the Contingency Module (CM) in case:

- Business continuity is impossible;
- Systemically important payments require to be processed during failing over.

CM used only during day-trade phase

CM should be activated immediately in case of SSP failure.

3 SSP failure - Contingency

Limiting payments eligible for contingency

- Technical limitations of CM

- Operational limitations

  - Contingency processing largely manual.
  - Input capacity varies across central banks depending on number of staff and logistics.
  - Some capacities for coordination and preparation of (re)opening of the SSP.

- Liquidity limitations (CM starts with zero balance)

3 SSP failure - Contingency

Very-critical payments (mandatory)

- Settlement payments from T2 to CLS
- Settlement payments from T2 to EURO1 for EoD
- Margin calls from T2 to CCPs

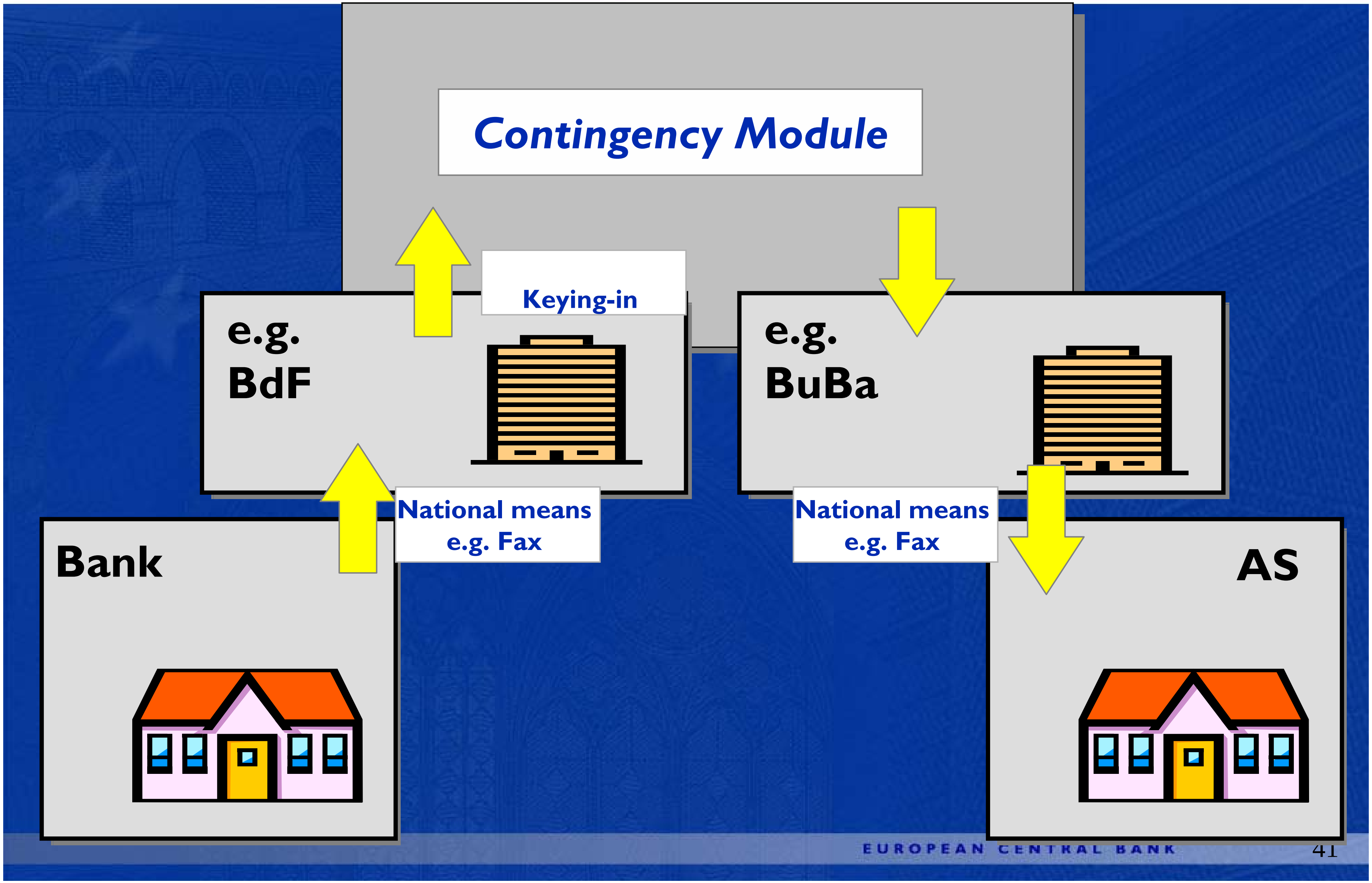
3 SSP failure - Contingency

Critical payments (optionally)

- Settlement payments for real-time settlement of interfaced SSS
- Additional outgoing payments to avoid systemic risk
- Incoming/liquidity (re)distributing payments if evidence that indispensable for (very)critical payments

(Crisis Manager assessment dependent on specific circumstances, failure duration etc) (> *see "List of aspects for crisis managers"* <)

3 SSP failure - Contingency



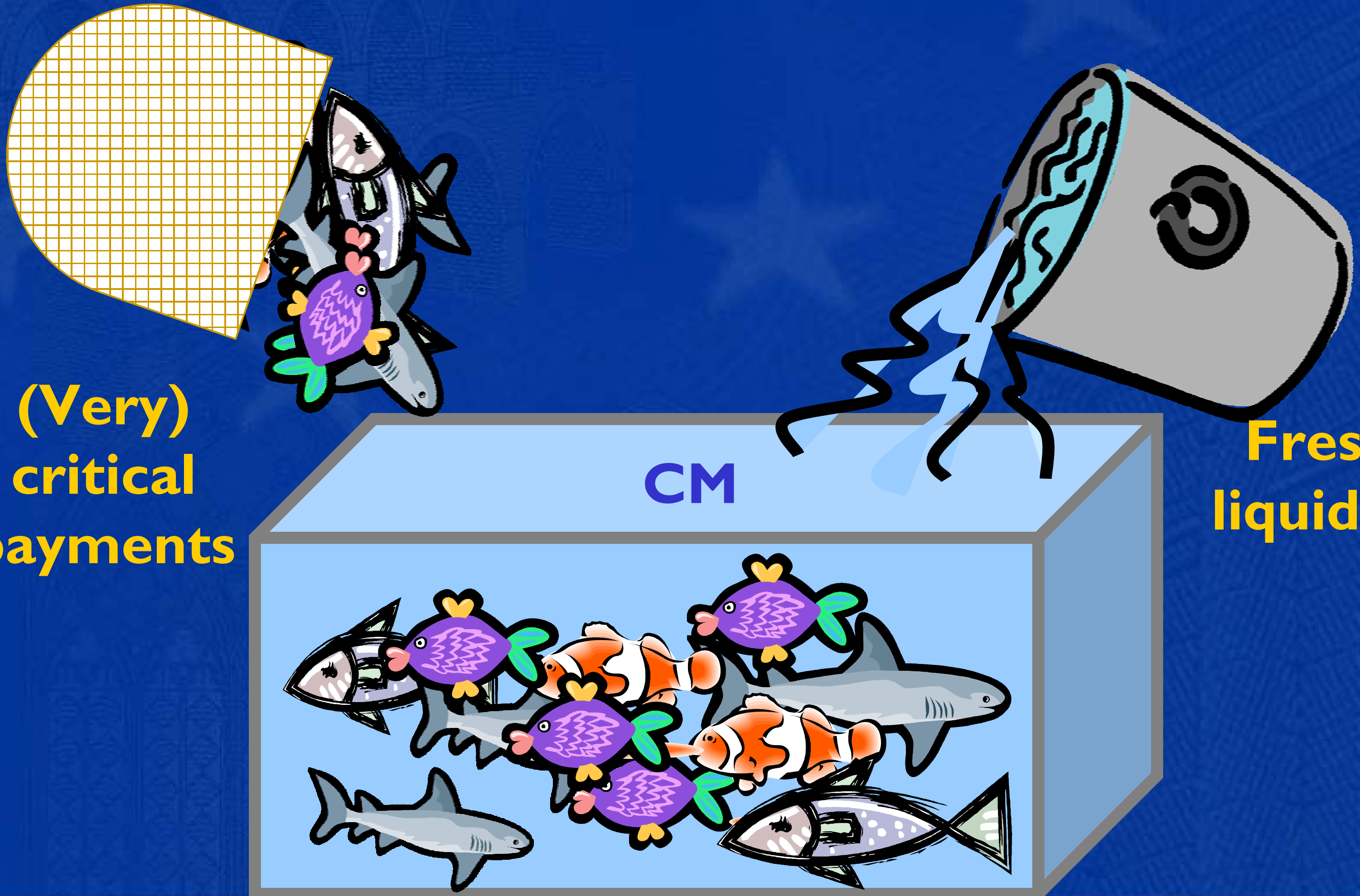
Need for fresh liquidity

CM starts with a zero balance. While payments capacity is blocked in the SSP, payments processing in the CM requires provision of fresh liquidity by means of:

- Additional collateral
- Contingency payments coming from AS (e.g. CLS pay-out)
- Received contingency payments

3 SSP failure - Contingency

Need for fresh liquidity



Need for fresh liquidity

Collateral management heterogeneous across euro-area (e.g. pledge or repo country)

Individualised follow–up:

Each CB in collaboration with its users has to ensure effective, operable and timely procedures for activation of additional collateral and fresh liquidity.

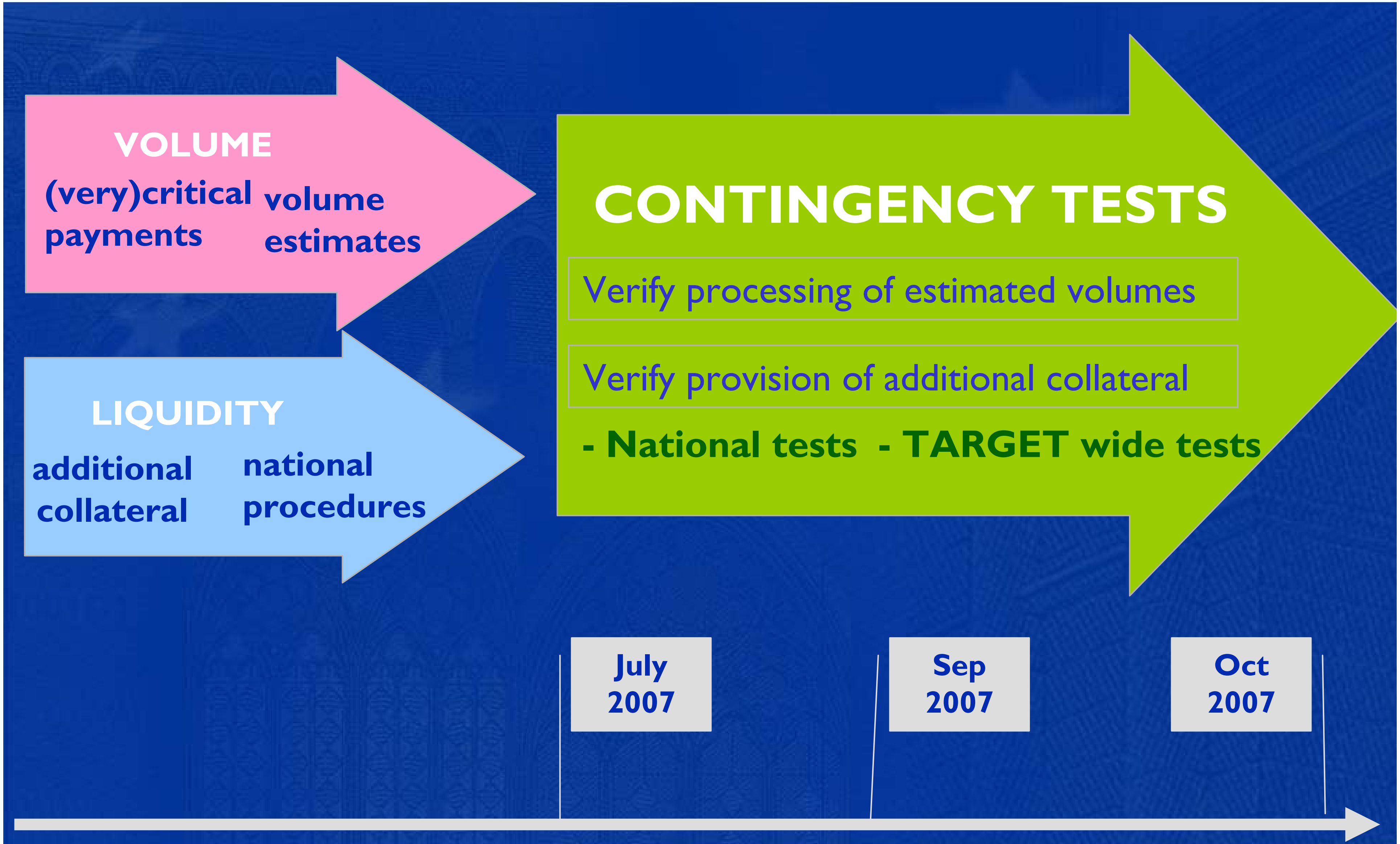
CM functionality

- Only interbank credit transfers
- CM provides limited functionality (no ”mini RTGS”)
- CB access CM via standard interface (runs in non-active Region)
- Communication sender – NCB, booking on accounts (accounts mirrored from PM without balances), communication NCB – beneficiary. Communication means dependent on national arrangements.
- No direct access of users to CM information. Information about turnover and account balances in the CM provided via the respective NCB.

CM functionality

- With the closing of the CM, the account balances are booked in the PM.
- Account holders are informed about the bookings optionally (MT940/950).
- For payments processed via the CM, the banks need to be aware that, if they send payments during the SSP failure to the SSP (which will be queued in the PM), these would get processed with the recovery of the SSP (risk of double processing).
- CM value date is bound to the value date of the SSP.

3 SSP failure - Contingency



VOLUME

(very)critical payments

volume estimates

LIQUIDITY

additional collateral

national procedures

CONTINGENCY TESTS

Verify processing of estimated volumes

Verify provision of additional collateral

- National tests - TARGET wide tests

5 SSP Failure

- Delayed Closing -

5 SSP failure – Delayed closing

Principles

- Delayed closing means extending the day trade phase.
- If a SSP failure struggles with EoD, there is <u>no alternative to a delayed closing.</u>
- A SSP failure solved before 6 pm might also lead to a delay (dependent on time of occurrence, duration).

3 SSP failure – Delayed closing

Principles

- TARGET2 should always close in a final manner >> processing of all payments on value day, i.e. no enforced closing
- During delay, users might still send messages to SSP, which would be stored at SWIFT level.

3 SSP failure – Delayed closing

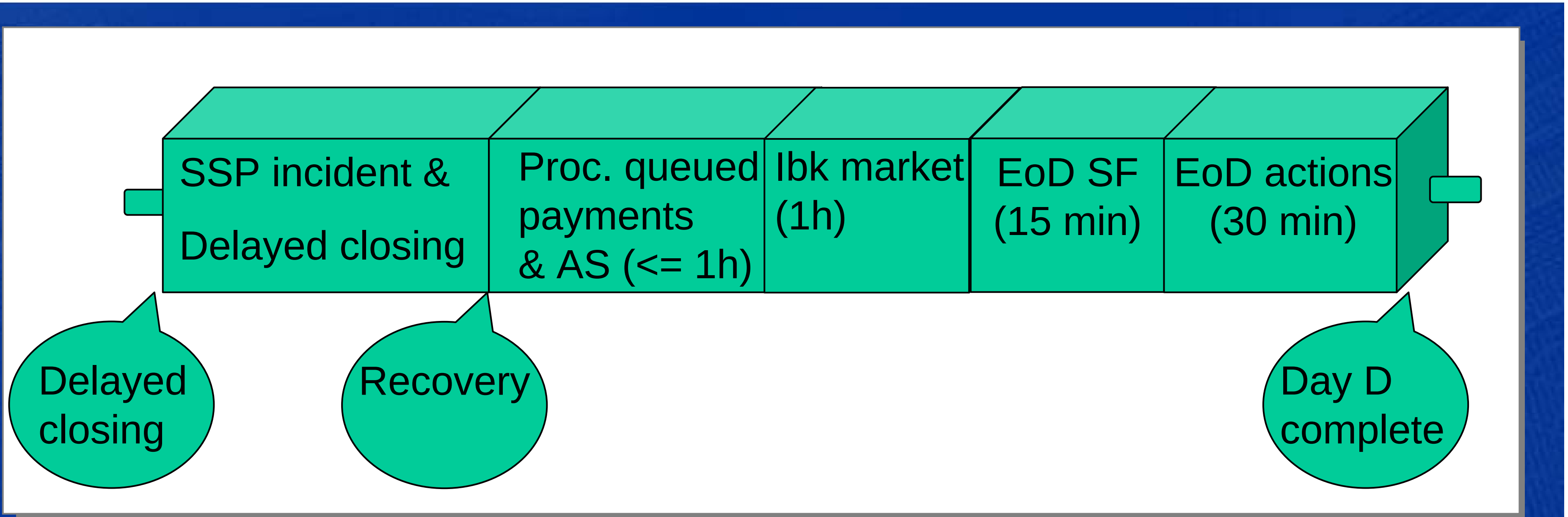
Principles

Banks, Ancillary systems and Central Banks have to ensure that they can cope with an exceptional long lasting delayed closing.

Delayed closing impacts on SCSS

- ICSDs might continue processing and change business day independent of SSP.
- CSD might follow the delayed closing times in order to provide collateral for the CM (FOP transactions).

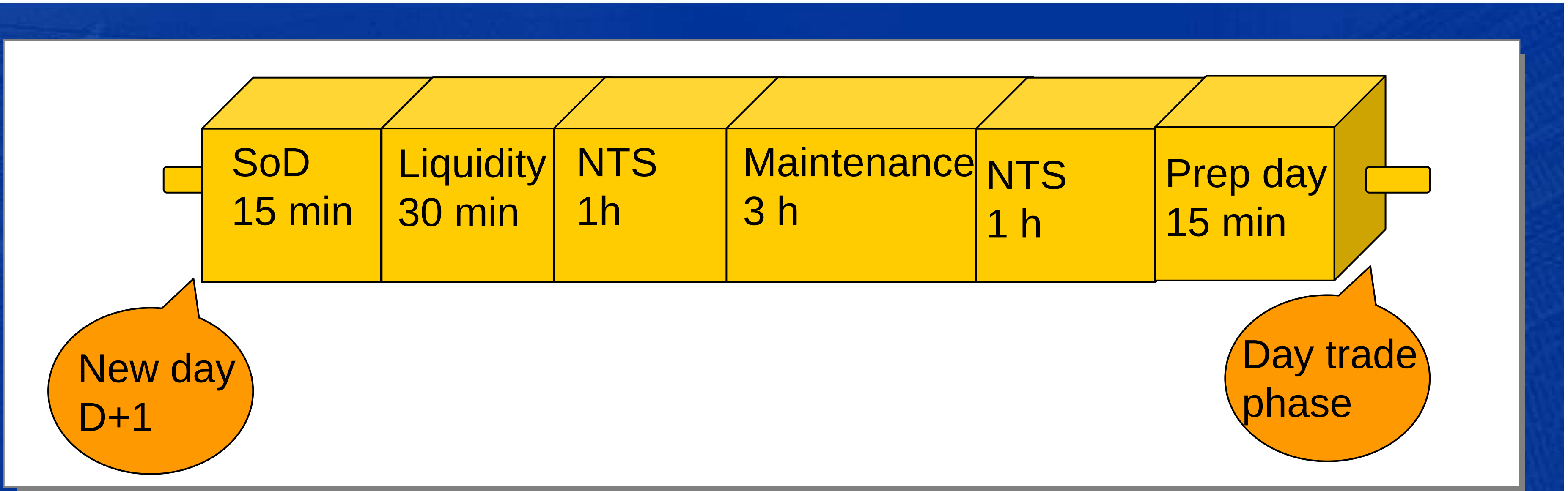
3 SSP failure – Delayed closing



SSP recovery is the moment in time, where the SSP is ready to process messages again.

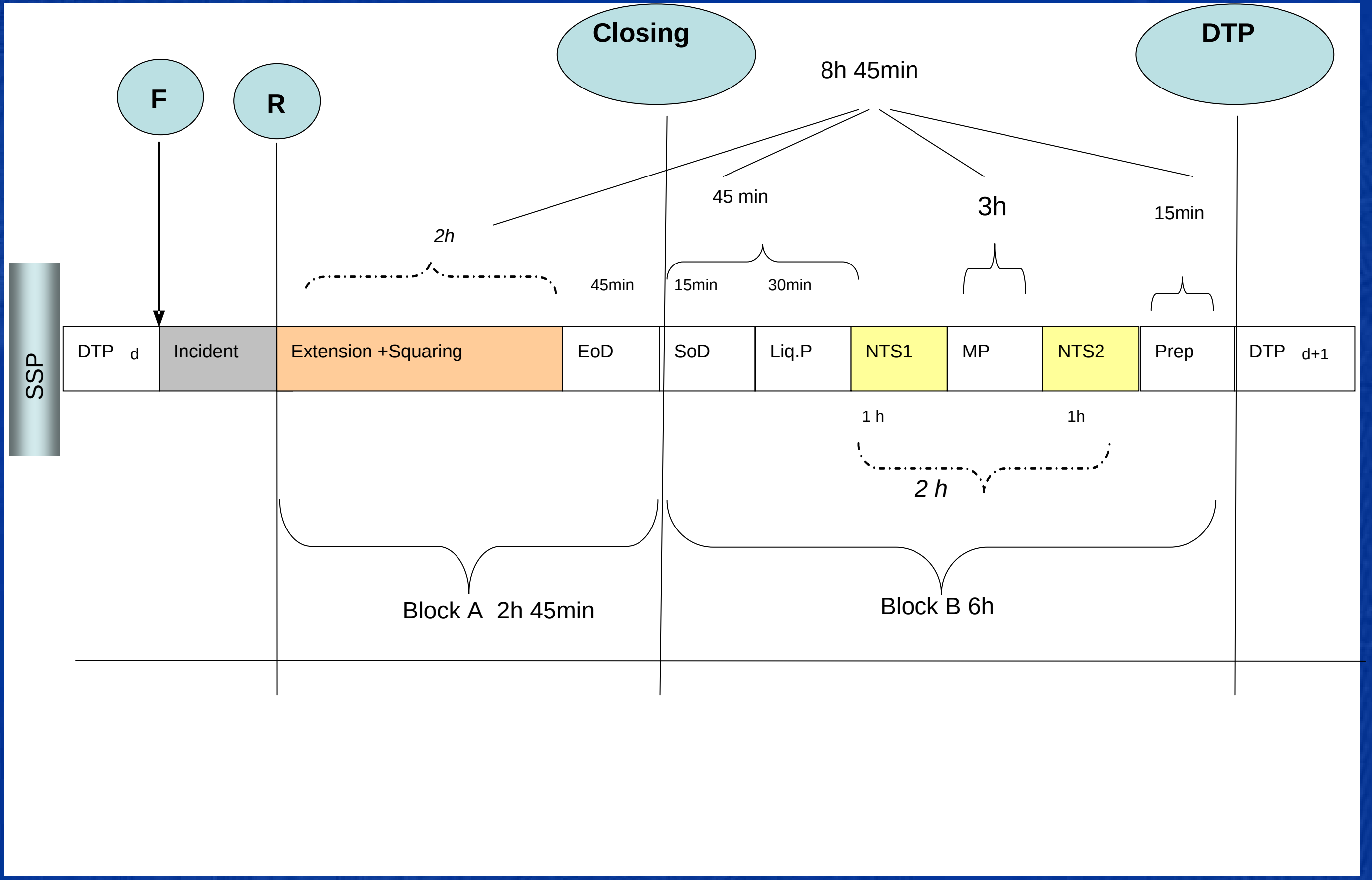
In total, 2 h 45 min required from recovery until the completion of day D.

3 SSP failure – Delayed closing



In total 6 h from start of day until the start of day trade phase required.

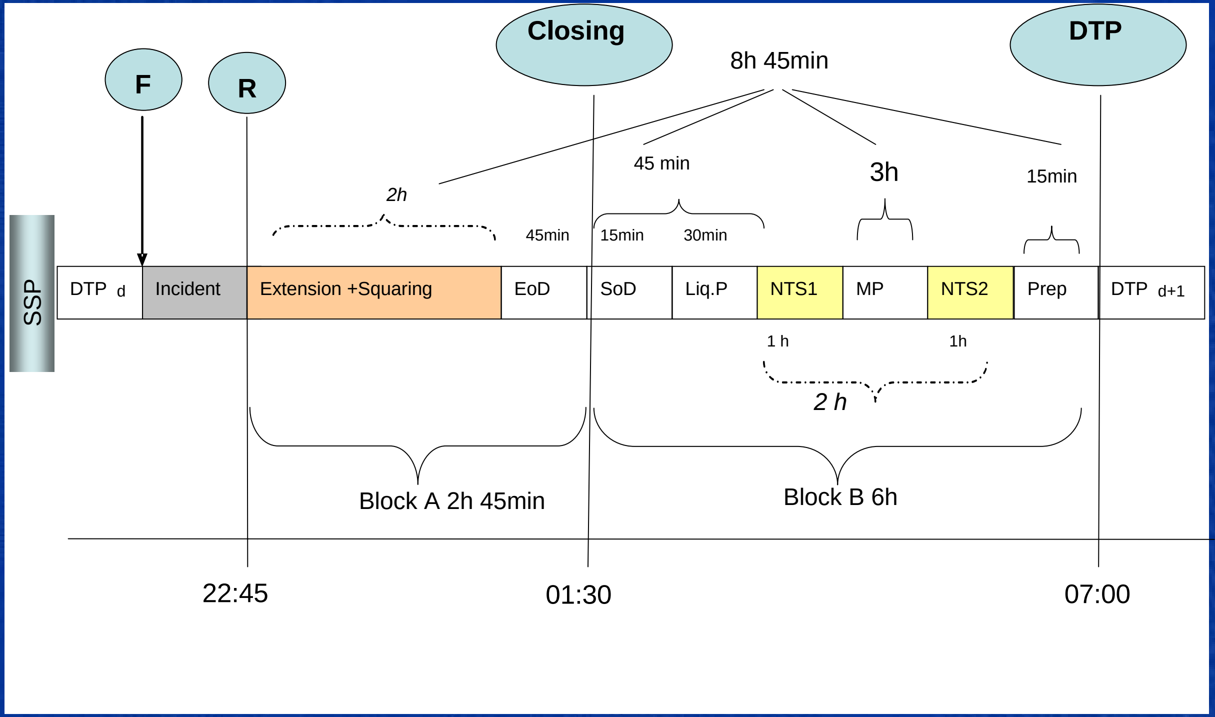
3 SSP failure – Delayed closing



Total time requirement from recovery until start of day trade phase: 8h45min

3 SSP failure – Delayed closing

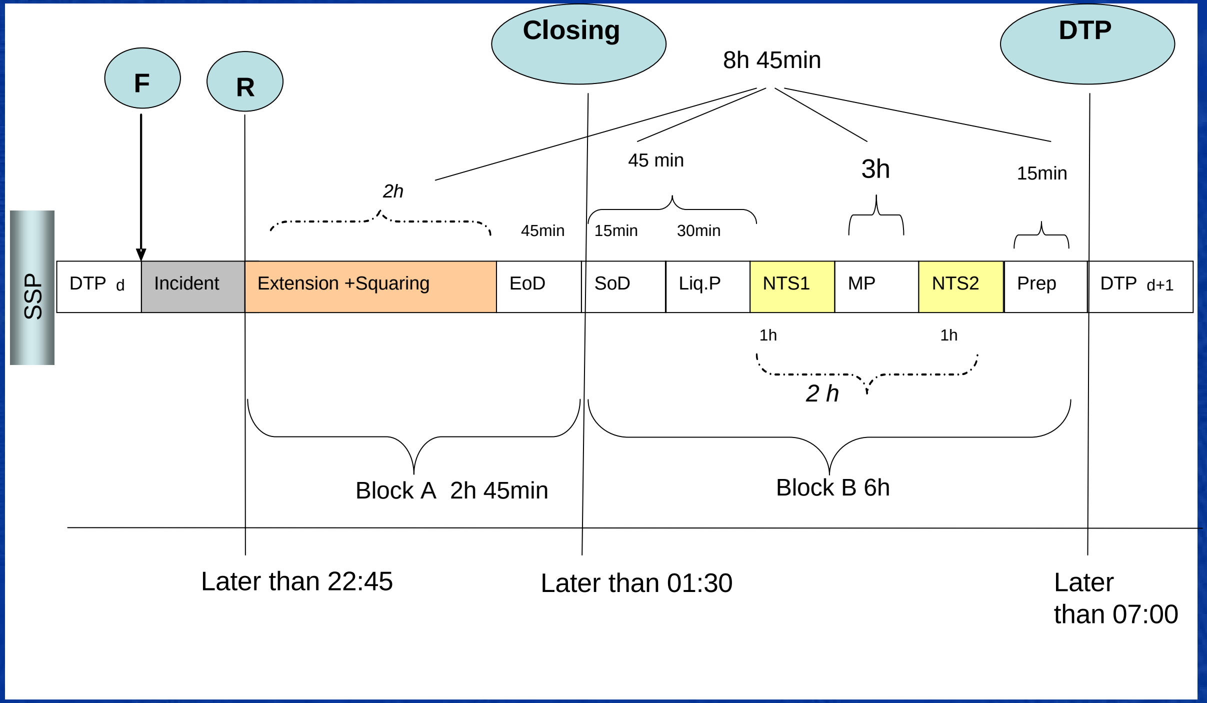
Scenario I



SSP recovers before 22:15, i.e. DTP can start normally at 07:00

3 SSP failure – Delayed closing

Scenario 2



SSP recovers after 22:15. A sequential running of the steps would delay the start of DTP at 07:00.

3 SSP failure – Delayed closing

Mandatory steps:

- **Completion of Day D (2 h 45 min)**
- **SoD, liquidity provision** (PM, HAM, PHA) **(45 min)**
- **Liquidity provision for NTS (1 h)**
- **Maintenance period (3 h)**

>>> Then open SSP for <u>both</u> DTP and NTS at the same time.

If timely/shortly delayed start of DTP unachievable, AS in need of EUR liquidity (e.g. CLS, CCP) need to refer to own arrangements or "wait" until start of DTP.

4 CB/PHA Failure

- *Each NCB will present its particular arrangements insofar these concern the users.*
- *A CB or PHA failure would of course still mean that the SSP is operating normally.*

4 CB/PHA failure

Principles

- **Limit impact on T2 to the extent possible**
- **Under responsibility of respective CB**
- **Use of national procedures** *(manual processing, workarounds, postponing operations)*
- **Central banks' backing up each other**
- **Exceptionally: Request T2 delayed closing**

5 Bank / AS Failure

5 Bank / AS failure

Principles

- First, use your own means. Only afterwards, use the support of the National Service Desk.
- Respective user to avoid spill-over effects to TARGET2. The “Measures to ensure security and operational reliability of T2 participants” addresses the users’ components security.
- Bank failure should never lead to a T2 delayed closing, AS failure only exceptionally.
- Relationship to users fully within national responsibility.

5.1 Bank Failure

5.1 Bank failure

Toolbox

1st own contingency means

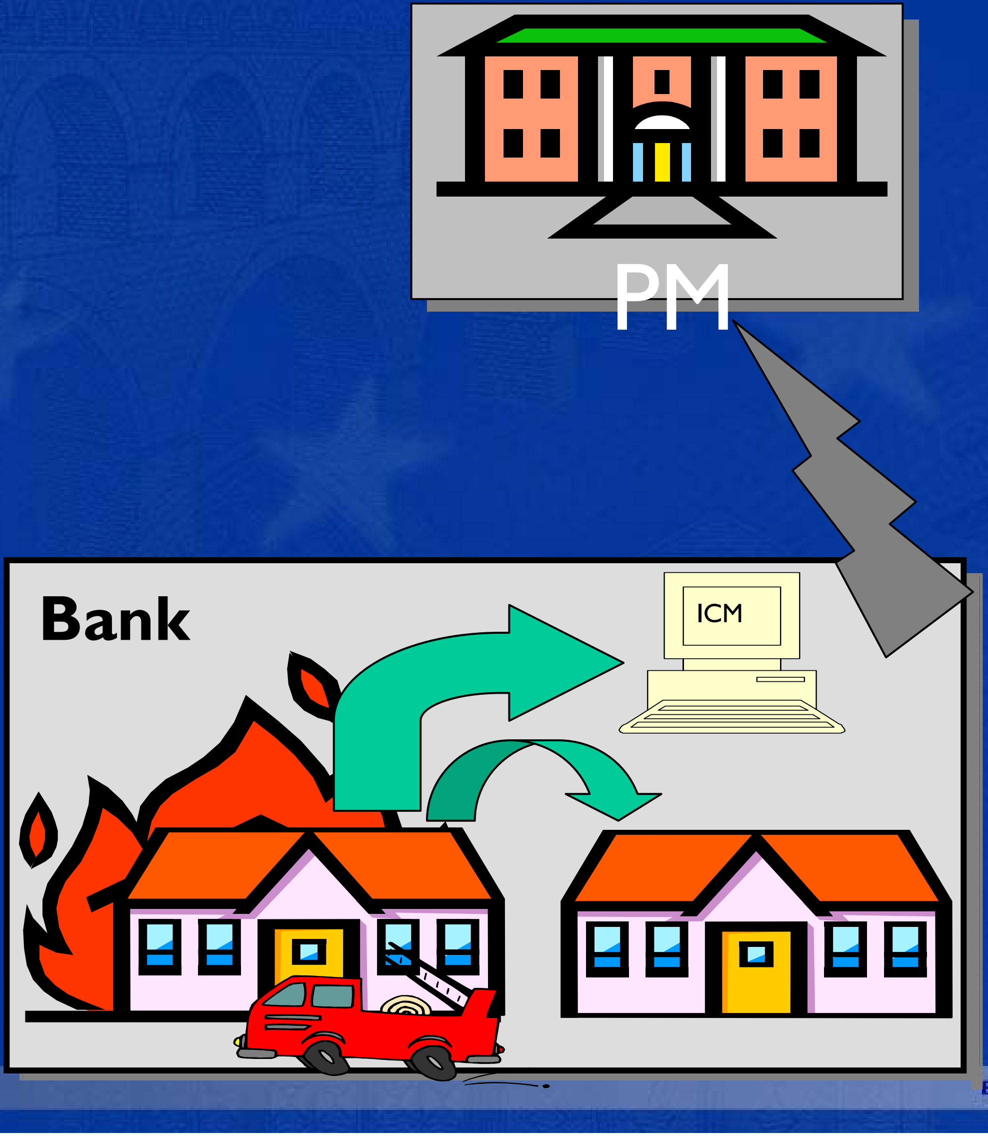
Inhouse solutions; ICM functionality, i.e. backup lump sum payments and backup contingency payments (CLS, EURO1, STEP2 pre-fund); ICM functionality via a stand alone ICM

2nd support of respective CB

National contingency means subject to relationship between bank and respective NCB

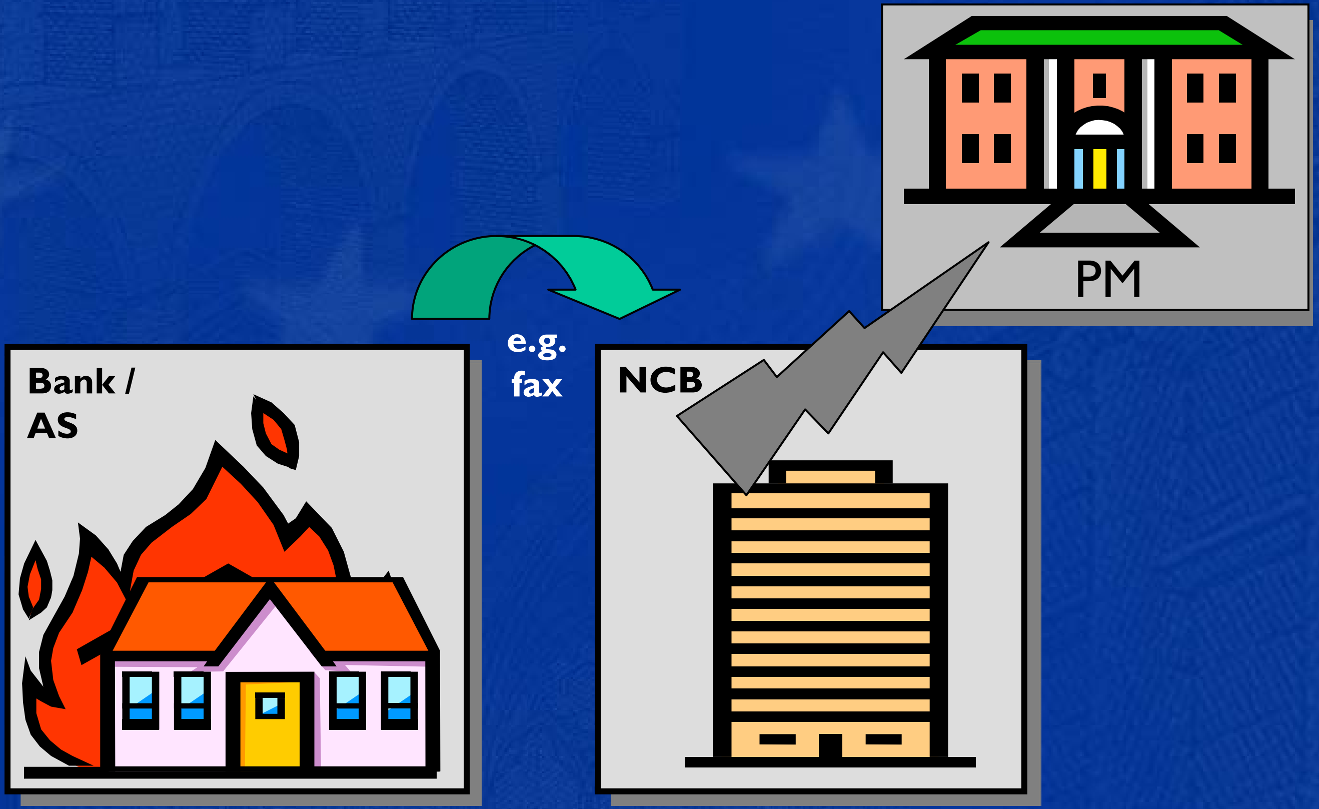
5.1 Bank failure

A user should first refer to its own tools



5.1 Bank failure

A user might also ask the National Service Desk for support.



5.2 Bank failure

On lump-sum payments

- Banks internal scheme (bank requests NCB to open lump-sum functionality)
- Follow-up on next days in banks’ discretion
- SSP does not verify whether original single payments were submitted or returned backup lump-sum payments are related to submitted payments of preceding days
- No check for double submission on preceding days
- Value date check switched off for participant and recipients of lump-sum payments

5.2 AS Failure

5.2 AS failure

Toolbox

Possible means for dealing with an event where the Ancillary System using the ASI is not able to:

- create XML messages to be sent to ASI;
- send XML messages to ASI.

  - Tools at the discretion of each AS!
  - Prearrangements and communication with users and Central Bank necessary!

5.2 AS failure

Toolbox

1st own contingency means

Back up side, multi-access points to multi-network partners to use normal means (e.g. ASI)**, as back up, possibly Payments Interface to SSP** (clean payments)

2nd support of respective CB

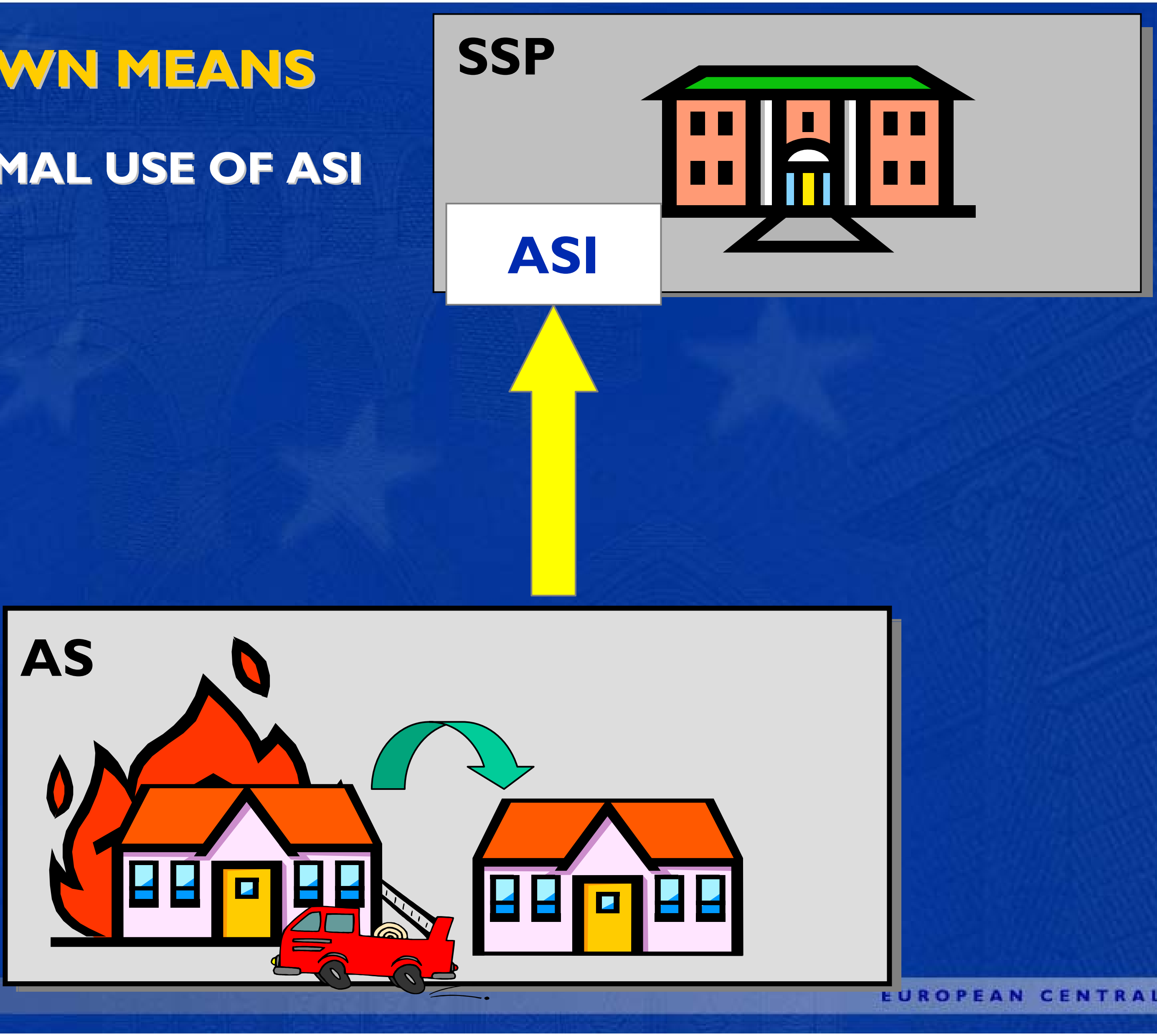
Some CBs offer to process XML files on behalf of the AS via the "*AS contingency tool*" or clean payments

Exceptionally: A T2 delayed closing might be requested for an AS failure

5.2 AS failure

OWN MEANS

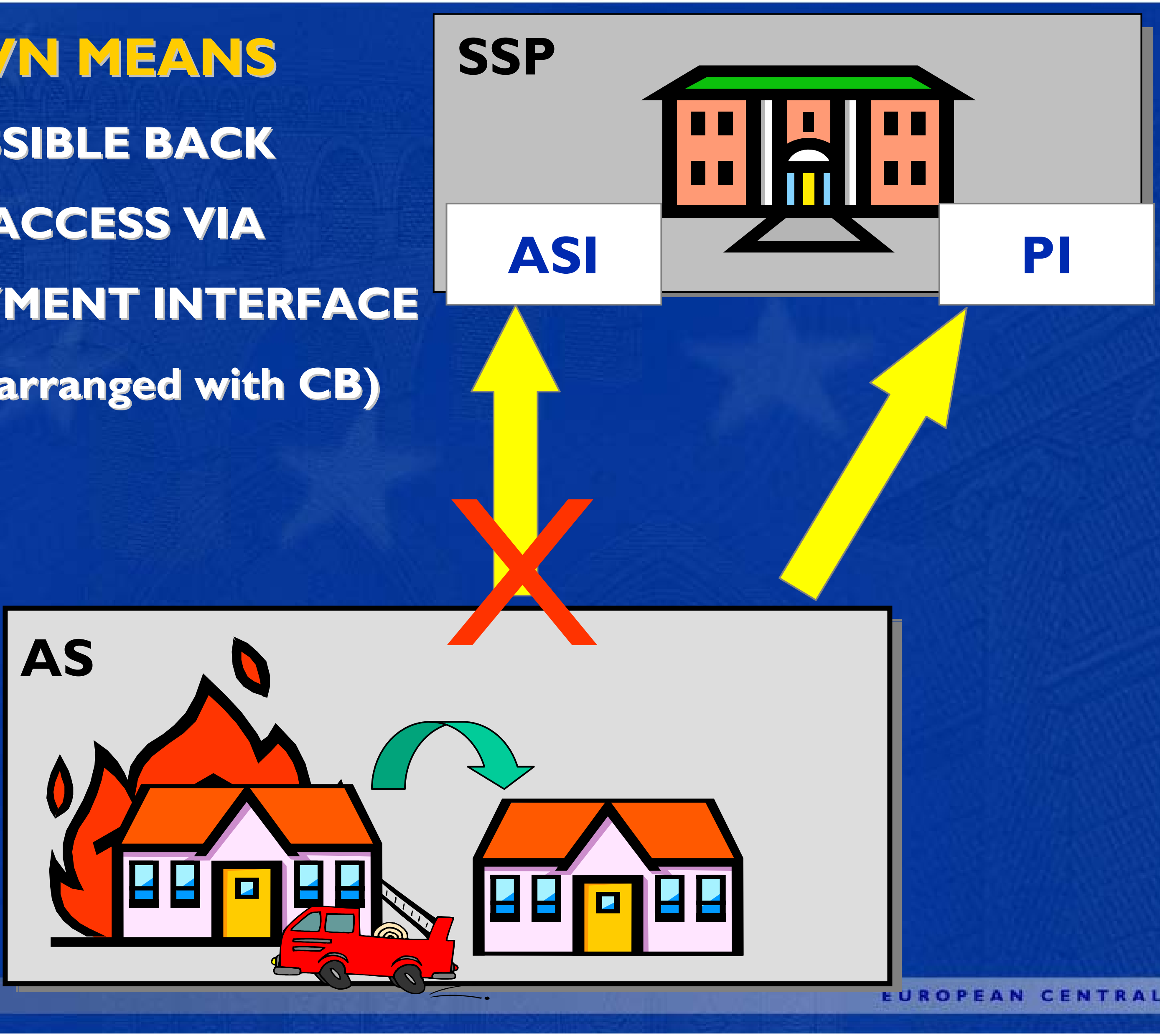
NORMAL USE OF ASI



5.2 AS failure

OWN MEANS

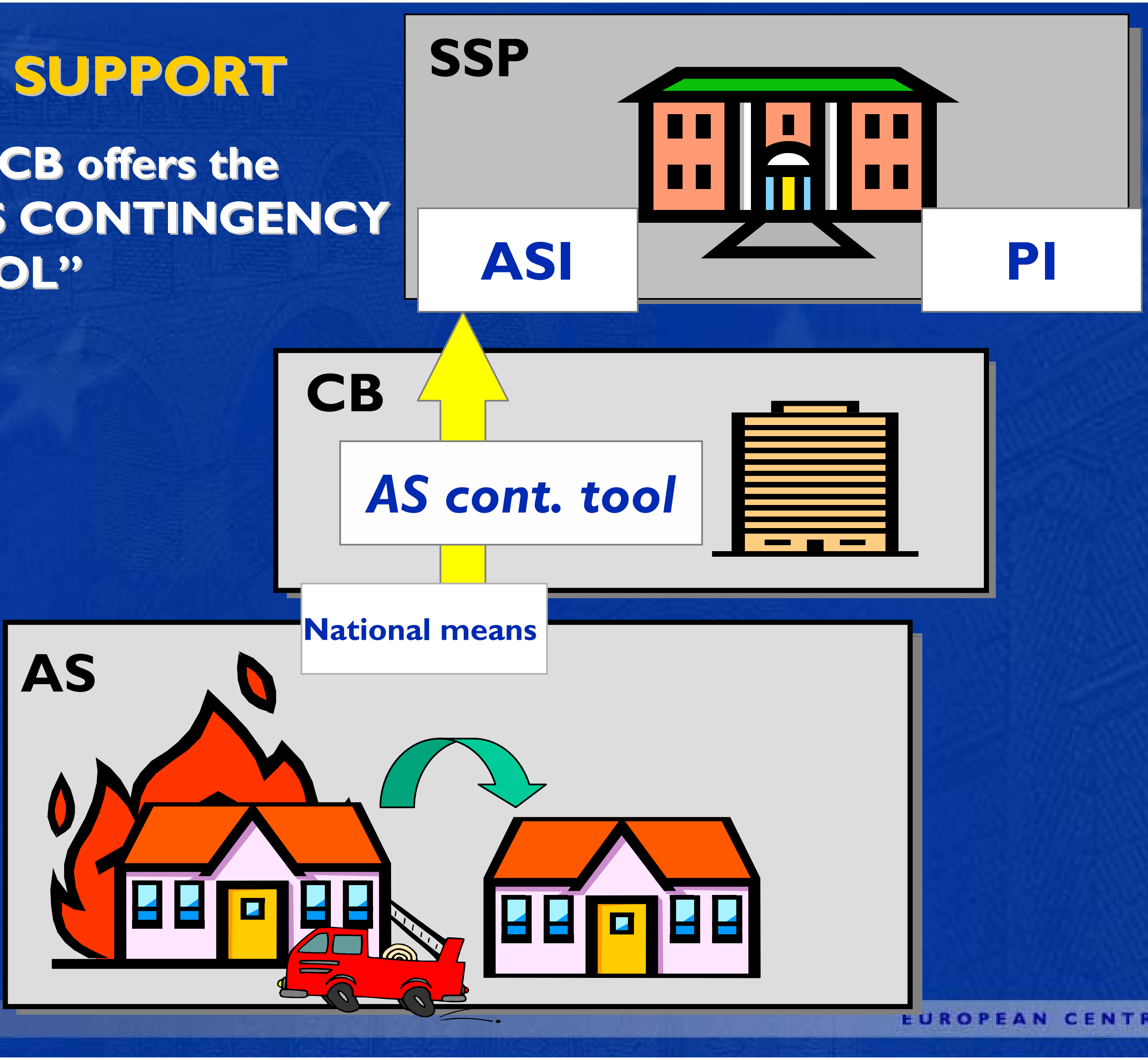
POSSIBLE BACK UP ACCESS VIA PAYMENT INTERFACE (prearranged with CB)



5.2 AS failure

CB SUPPORT

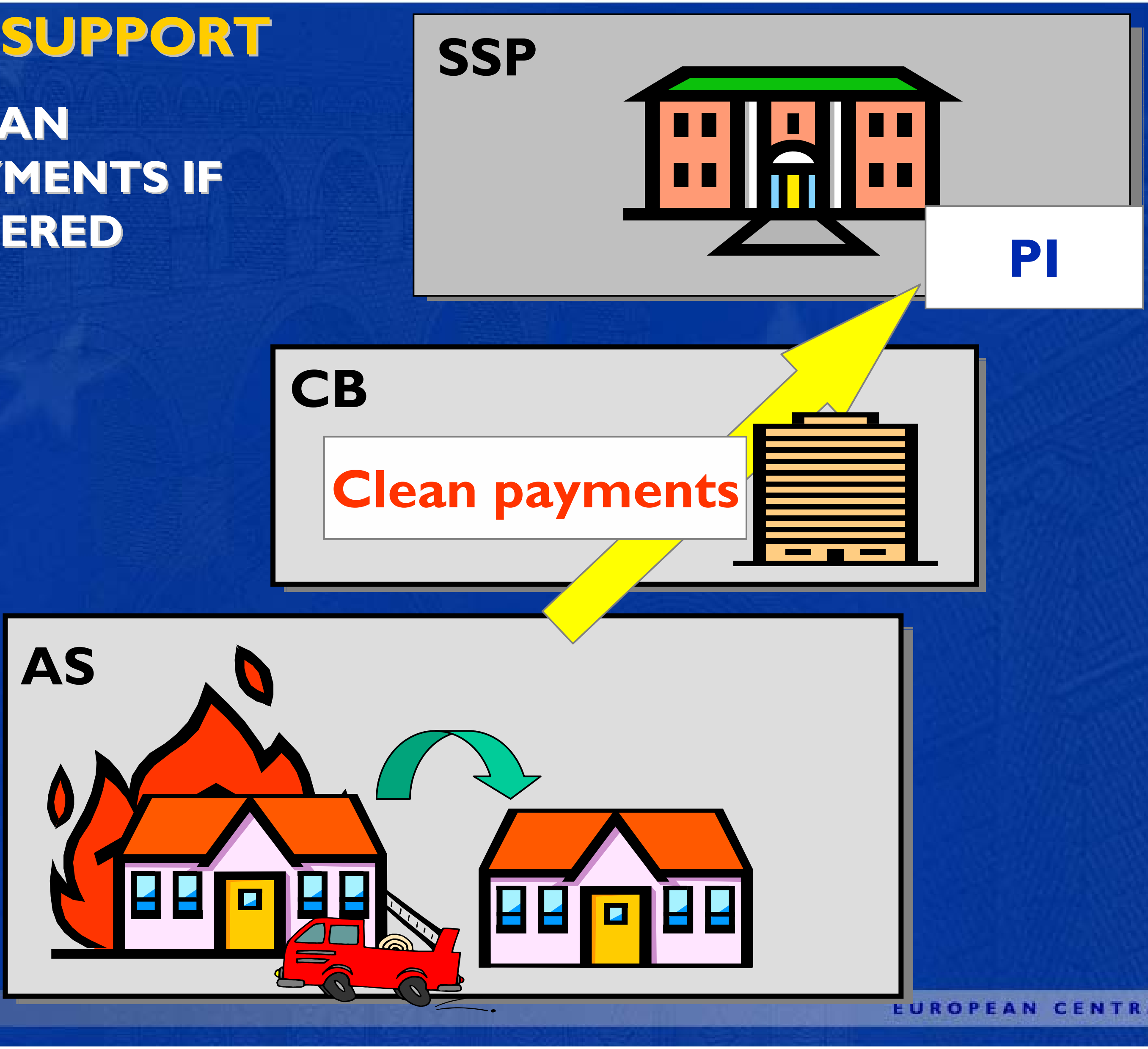
If NCB offers the "AS CONTINGENCY TOOL"



5.2 AS failure

CB SUPPORT

CLEAN PAYMENTS IF OFFERED



6 SWIFT failure

6 SWIFT failure

- TARGET2 builds on the resilience of SWIFT in view of global SWIFT outage
- Service commitments in view of recovery times
- SSP infrastructure itself would still be available
- Processing of (very)critical payments in the PM possible – on request of Crisis Managers

Thanks