ZABBIX 2015 Conference

5th annual Zabbix Conference

11 - 12 September 2015 | Riga, Latvia

share your passion and search for new knowladge

Pre

My timing starting from 20:00 11.09

20:00 – 24:00 – awesome party

24:00 – 02:00 – awesome Riga peoples

Pre

My timing starting from 20:00 11.09

20:00 – 24:00 – awesome party

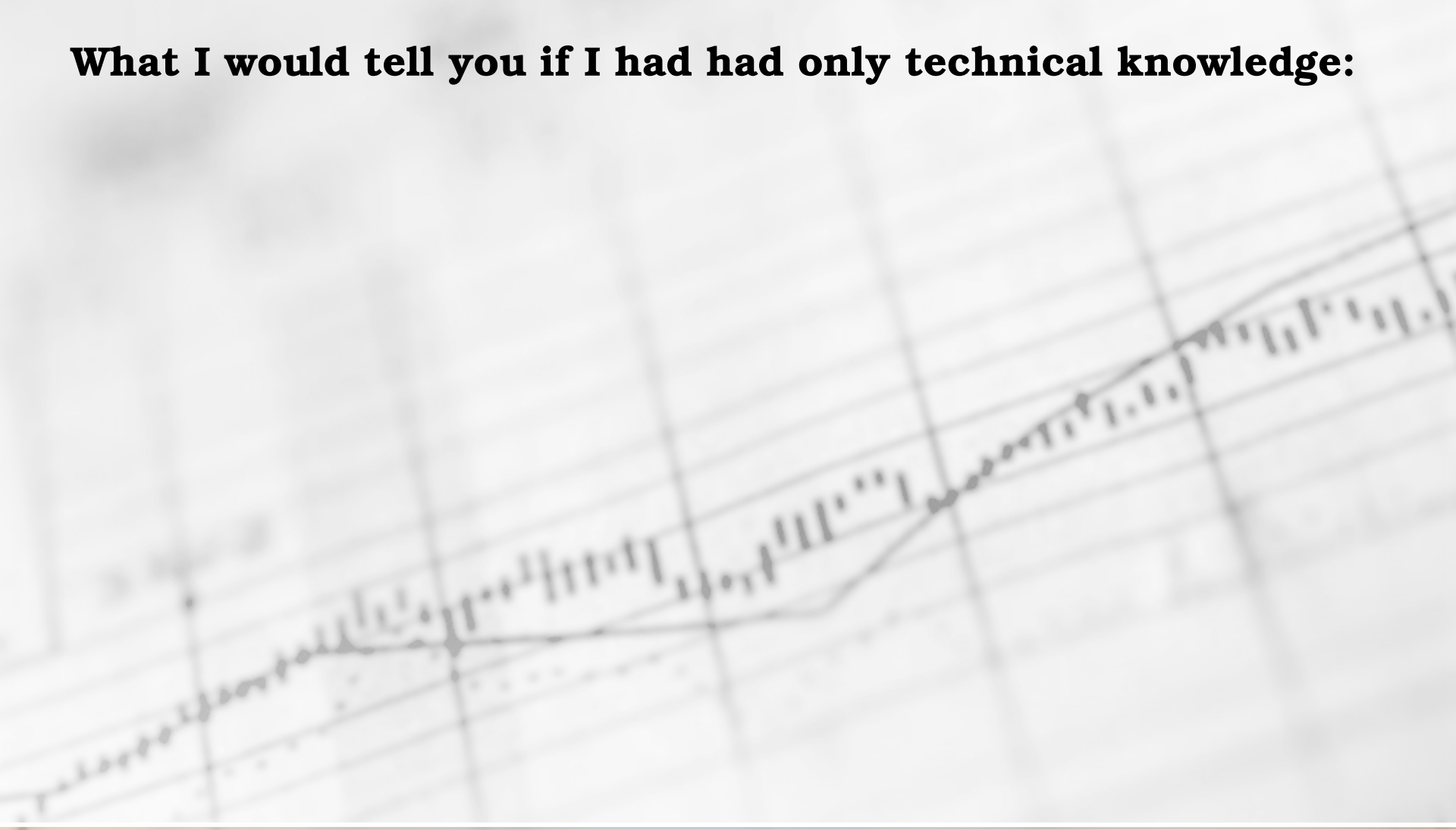
24:00 – 02:00 – awesome Riga peoples

07:21 – first critical SMS from zabbix

…a than - help ops & devs

Thanks to Zabbix team! =)

What I would tell you if I had had only technical knowledge:



What I would tell you if I had had only technical knowledge:

Event-driven

1. **Service discovery**

What I would tell you if I had had only technical knowledge:

Event-driven

1 **Service discovery**

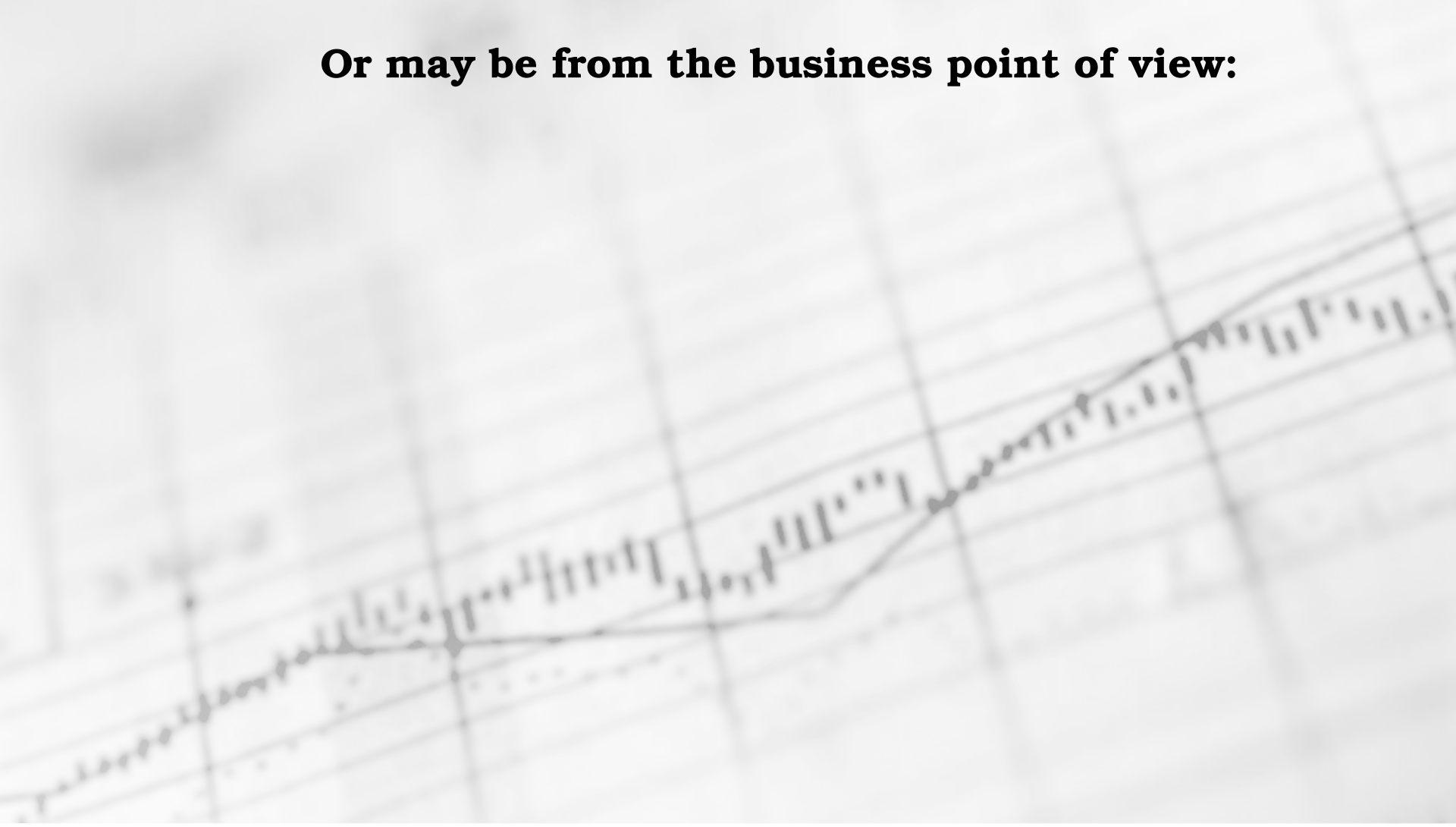
or

"receive, parse and store multitude of servers/services/data-flows, metrics, logs and actions in order to have an Mesos\Consul\etcd-like service register & discovery"

Eugene Istomin
IT Architect

e.istomin@edss.ee
Cone Center,Tallinn

Or may be from the business point of view:



Or may be from the business point of view:

Business continuity and the value delivery

2

Or may be from the business point of view:

Business continuity and the value delivery

2

or

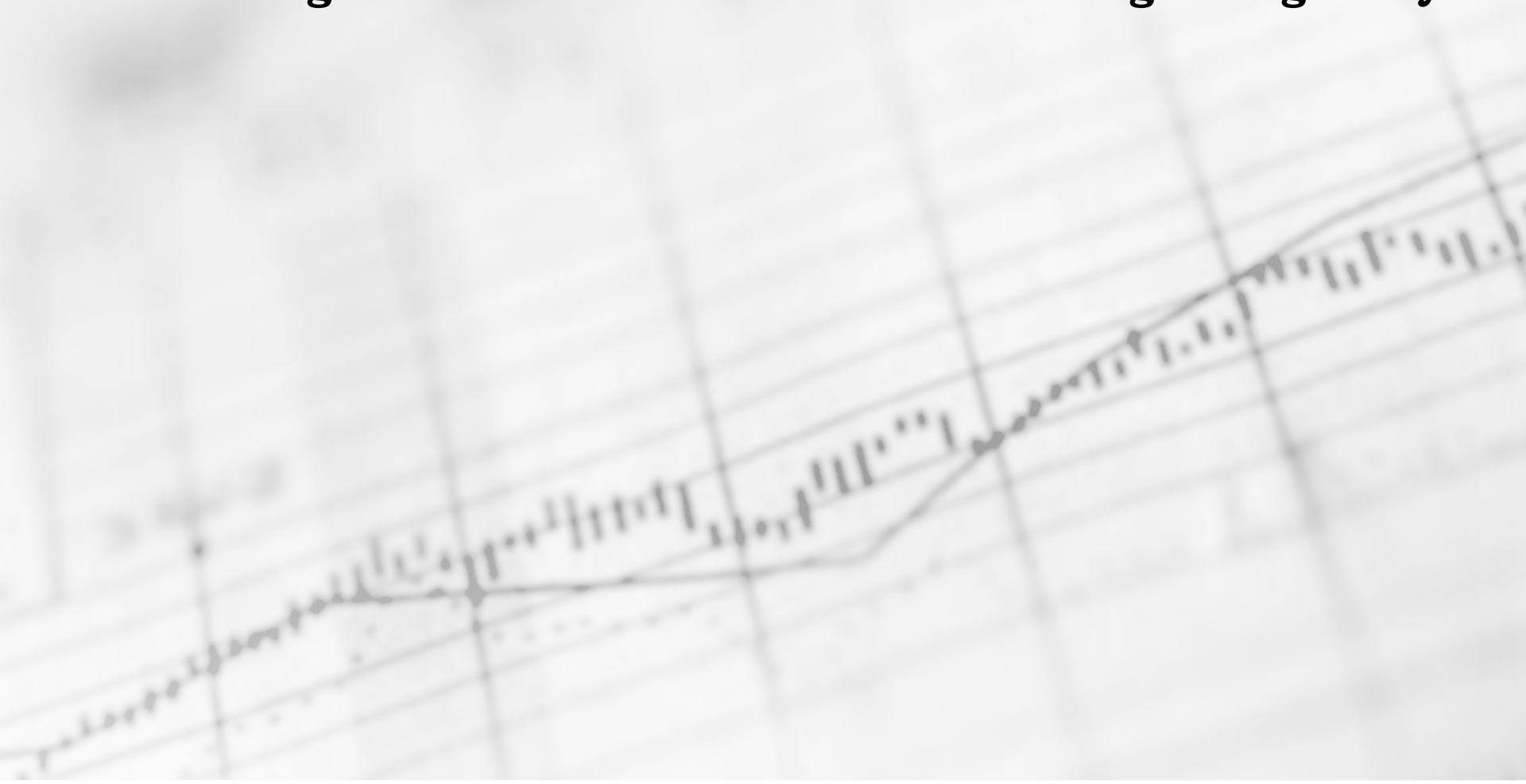
"what is the real cost of
resilience, recovery and contingency"

"risk management on steroids for 6-sigma value delivery"

Eugene Istomin
IT Architect

e.istomin@edss.ee
Cone Center,Tallinn

The knowledge artifact I have now is about the logitoring lifecycle:



The knowledge artifact I have now is about the logitoring lifecycle:

Architecture-driven

logitoring lifecycle

The knowledge artifact I have now is about the logitoring lifecycle:

Architecture-driven logitoring lifecycle

or

"please, no more another ugly DevOps logging and monitoring pattern"

the meaning of "logitoring" in architecture-driven logitoring lifecycle

Eugene Istomin
IT Architect

Cone Center

e.istomin@edss.ee
Cone Center,Tallinn

Background to

Logging & monitoring

or *logitoring*

"Time-machine to the

Zabbix Conference 2014"

Do the data in monitoring have

the same nature as data in logging?

IT Monitoring - sum of methods used to collect defined metrics using checks.

Monitoring ~ protocol/agent, desired data descr, centralized storage, notifications

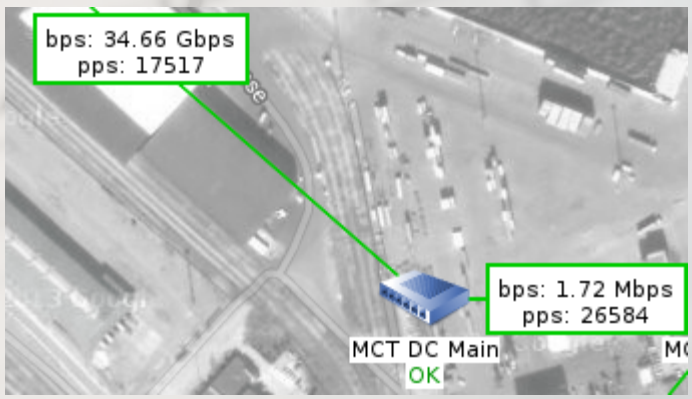
= Reactive

What is the classical monitoring metric?

Numeric! (int/bool/etc)

Monitoring is usually used for:

- Servers status dashboard creation
- IT-administrators notification
- Numeric info visualization
- IT-inventory



Monitoring In brief:

- Schema-based
- Use common network protocols or agents
- Stored data not reusable
- Needs by IT eng./admins

IT Logging - sum of methods used to collect pass-through flows information.

Logs ~ syslog, pid/severity/ program, transport, centralized storage.

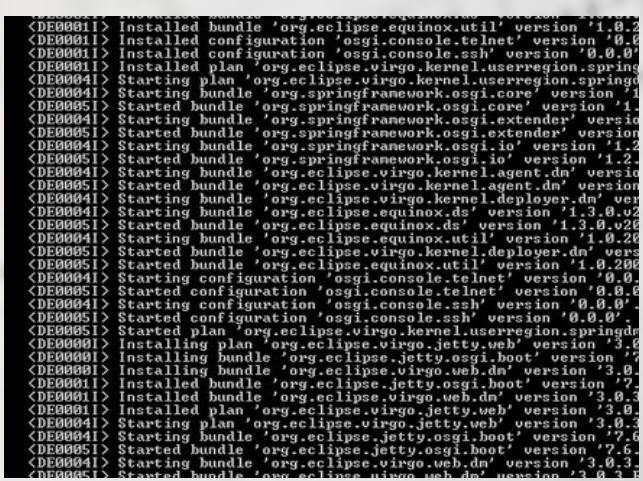
= Proactive

What is the classical logs metric?

String!

Logging is usually used for:

- Problem resolving
- Debugging & development
- Security access violation events storage



Logging In brief:

- Schema-less
- Use syslog or API/REST
- Stored data are reusable
- Needs by developers

Do the data in monitoring have the **same** nature as data in logging?

Yes,

- Monitoring and logging are subsets of **events**
- Monitoring is mainly **reactive**
- Logging is mainly **proactive**

Events is a set includes all possible types of messages (monitoring, logging, JSON data exchange by HTTP or TCP, etc)

Background to

enterprise architecture

and systems engineering

"Complexity is not an objective factor but a subjective one."

What is the #enterprise architecture ?

A **well-defined practice** for conducting enterprise

- analysis
- design
- planning
- implementation

What is the #enterprise architecture ?

A **well-defined practice** for conducting enterprise

- analysis
- design
- planning
- implementation

using a holistic approach at all times

for the **successful development** and **execution of strategy**.

What is the #enterprise architecture ?

Background to

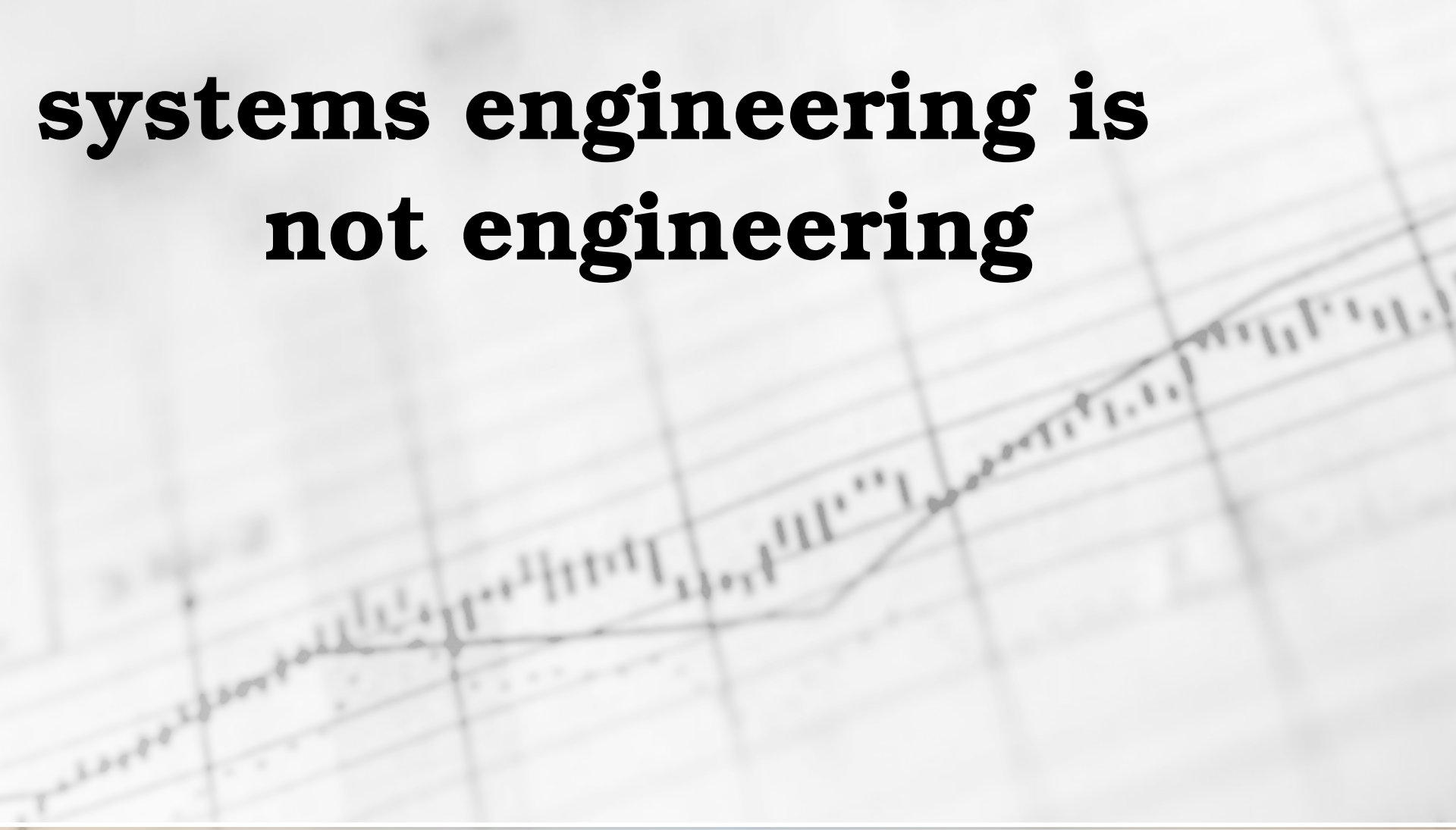
enterprise architecture

and systems engineering

"If we want to solve problems effectively...we must keep in mind not only many features but also the influences among them"

What is the #systems engineering ?

systems engineering is not engineering



What is the #systems engineering ?

systems engineering is
not engineering

What?

What is the #systems engineering ?

SE is a **technique** of using knowledge from **various branches** of **engineering** and **science**

What is the #systems engineering ?

SE is a **technique** of using knowledge

from **various branches**

of **engineering** and **science**

to introduce

technological **innovations** into the

planning and **development** stages of a system.

What is the #systems engineering ?

Business Process of TOGAF

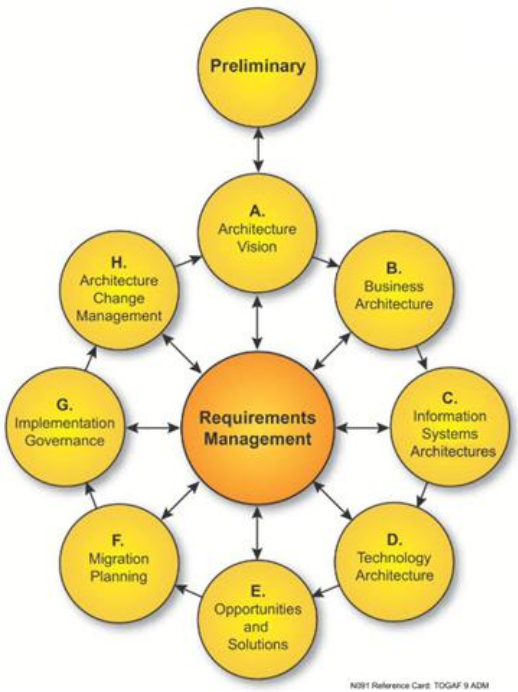


FIGURE I

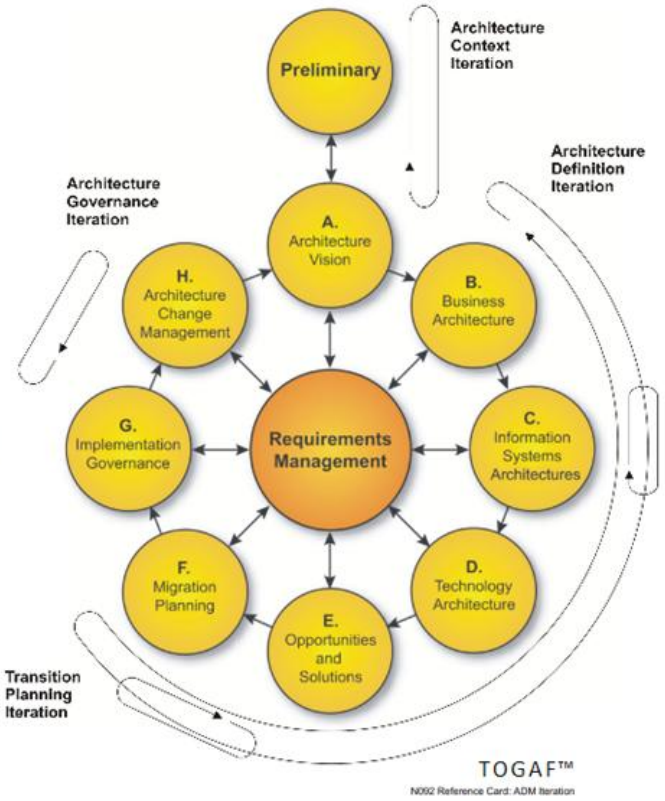


FIGURE II

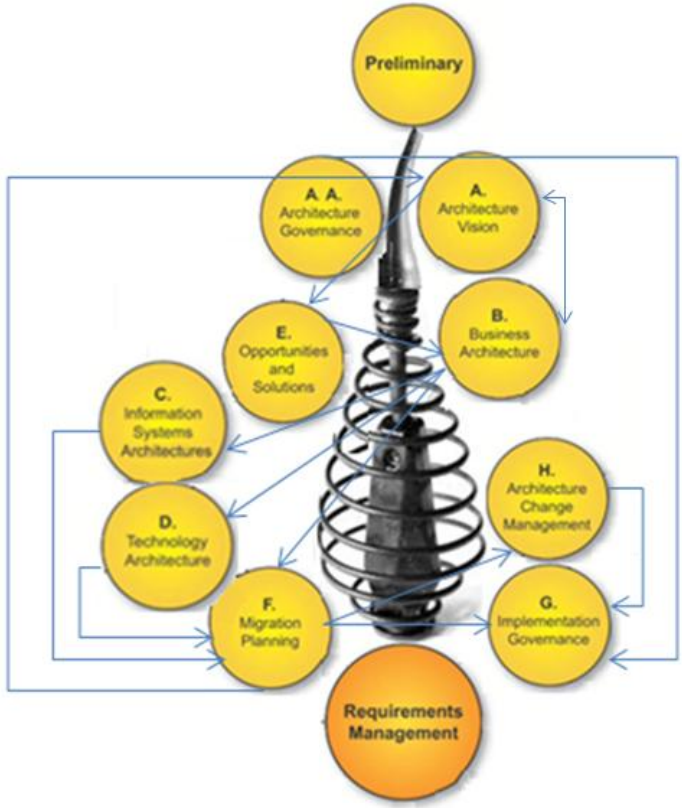


FIGURE III

Business Process of TOGAF

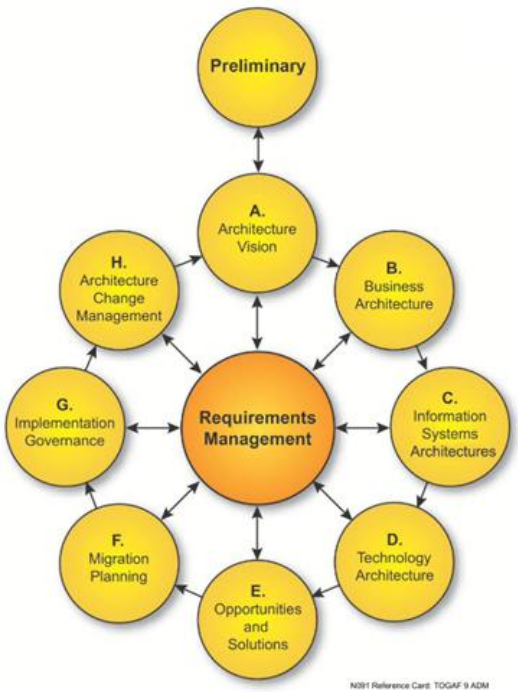


FIGURE I

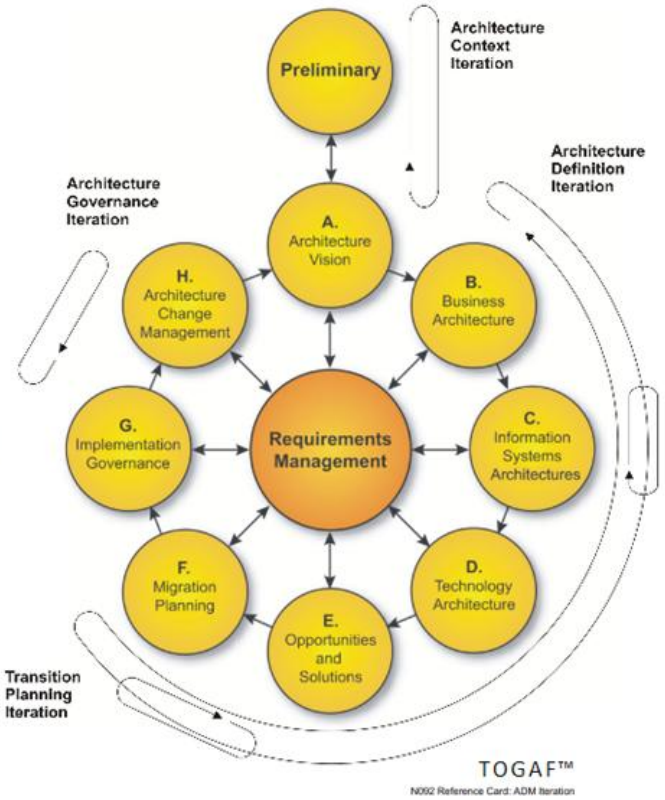


FIGURE II

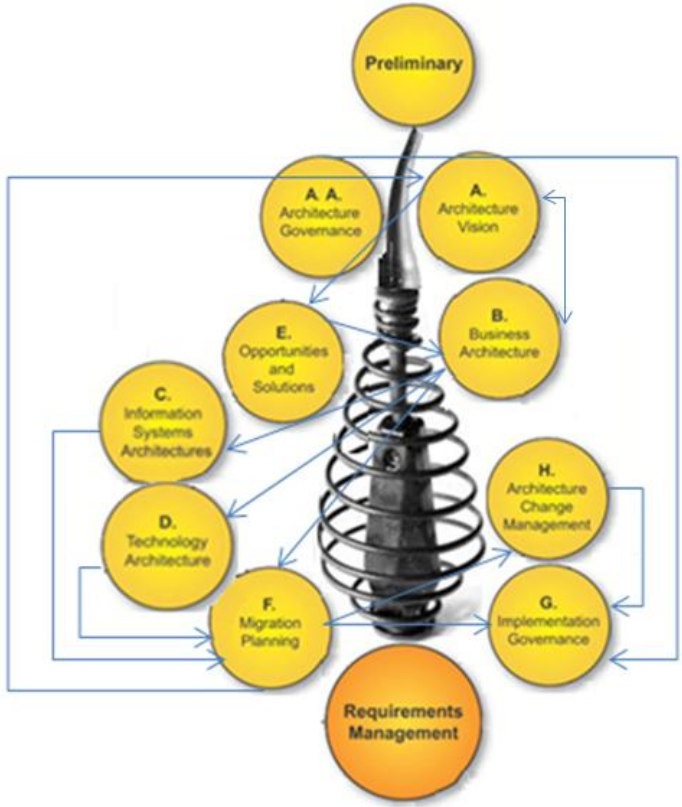


FIGURE III

…process is not that simple as appears in the TOGAF diagram even with flattened iterations.

Background to

enterprise architecture

and systems engineering

"TOGAF provides a best practice framework for adding value, and enables the organization to build workable and economic solutions which address their business issues and needs."

What is the #maturity model for enterprise architecture ?

5 levels and :

Administration – Governance Roles & Responsibilities

Planning – EA program road map and implementation plan

Framework - ..

Blueprint - ..

Communication - ..

Compliance - ..

Integration - ..

Involvement - ..

What is the #maturity model for enterprise architecture ?

5 levels and :

Administration – Governance Roles & Responsibilities

Planning – EA program road map and implementation plan

Framework - ..

Blueprint - ..

Communication - ..

Compliance - ..

Integration - ..

Involvement - ..

EA level 0

What is the #maturity model for enterprise architecture ?

5 levels and :

Administration – Governance Roles & Responsibilities

Planning – EA program road map and implementation plan

Framework - ..

Blueprint - ..

Communication - ..

Compliance - ..

Integration - ..

Involvement - ..

EA level 0

No rules at all =)

What is the #maturity model for enterprise architecture ?

5 levels and :

Administration – Governance Roles & Responsibilities

Planning – EA program road map and implementation plan

Framework - ..

Blueprint - ..

Communication - ..

Compliance - ..

Integration - ..

Involvement - ..

EA level 5

… Captured metrics are used to identify inefficiencies in

EA processes and templates prior to notification of issues

What is the #maturity model for enterprise architecture ?

What we have in real IT?

Just a some template without a common sense.

Background to

enterprise architecture

and systems engineering

Layers:

- *Business & Information*
- *Application & Data*
- *Technical Infrastructure*

Let's talk about #Archimate modelling

Archimate

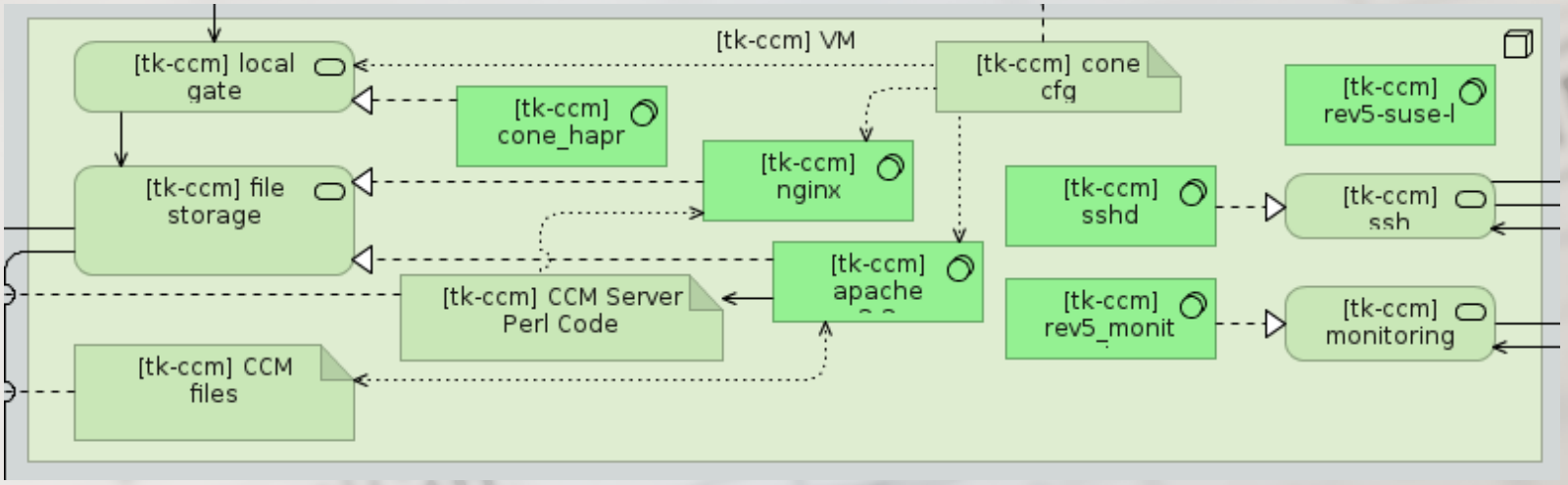
open and independent modelling language for enterprise architecture

ArchiMate provides

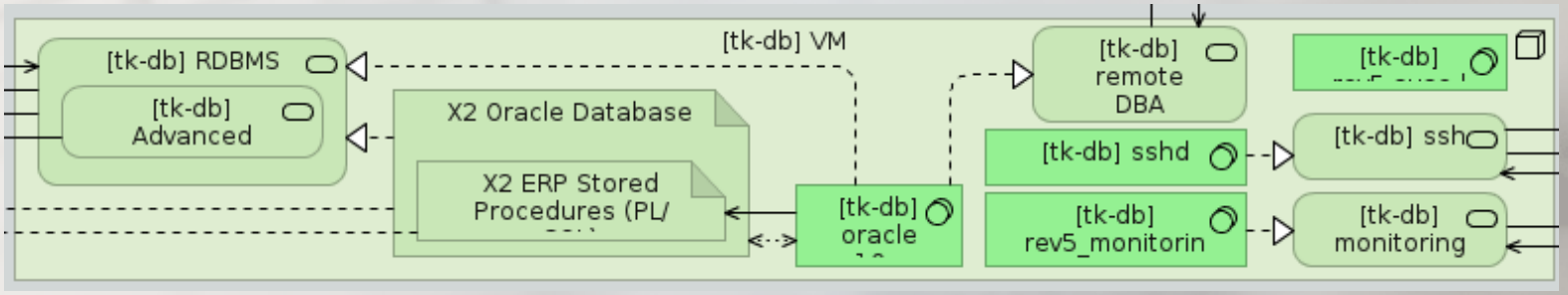
instruments to enable enterprise architects to describe, analyze and visualize the relationships among business domains

Let's talk about #Archimate modelling

Real Archimate scheme



From SSH/Zabbix on the right side
to application functions on the left side



Logitoring

Architecture-driven

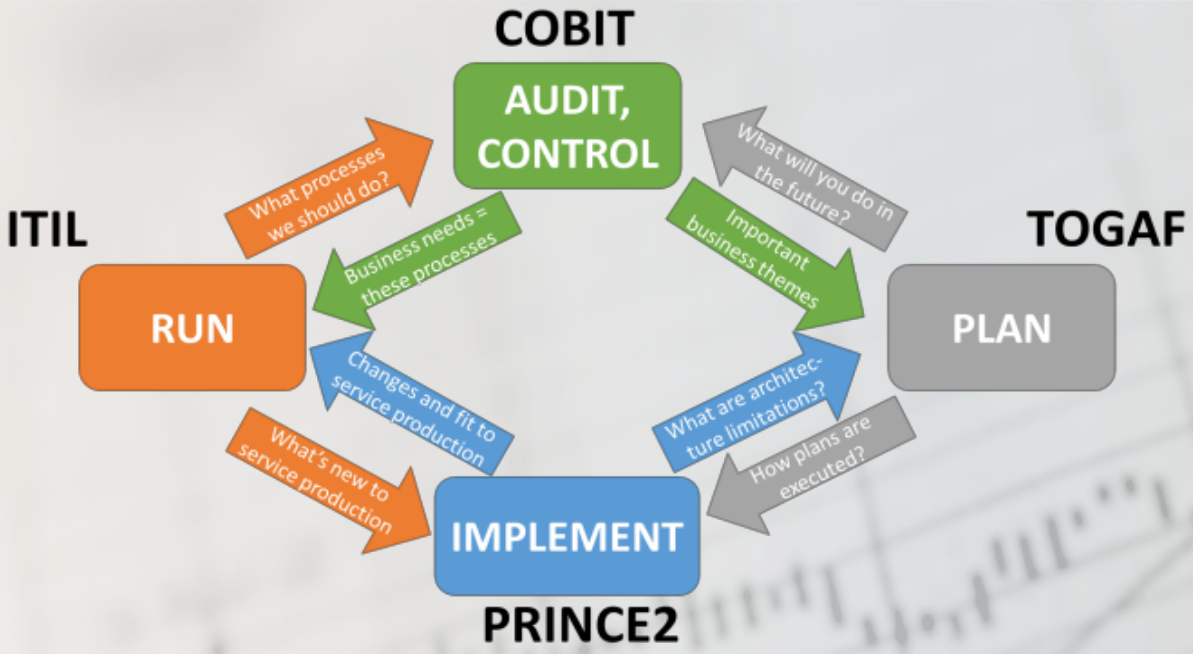
logitoring lifecycle

"The matter of logitoring
is events/facts provision
to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore -
Both are just the functions of the event provision engine"

What is wrong with monitoring & logging now?

Problems in Communication Between Popular IT Frameworks



"I been introduced to multiple different IT frameworks …

but they **all failed to capture the whole picture**."

Colour represent the way thinks:

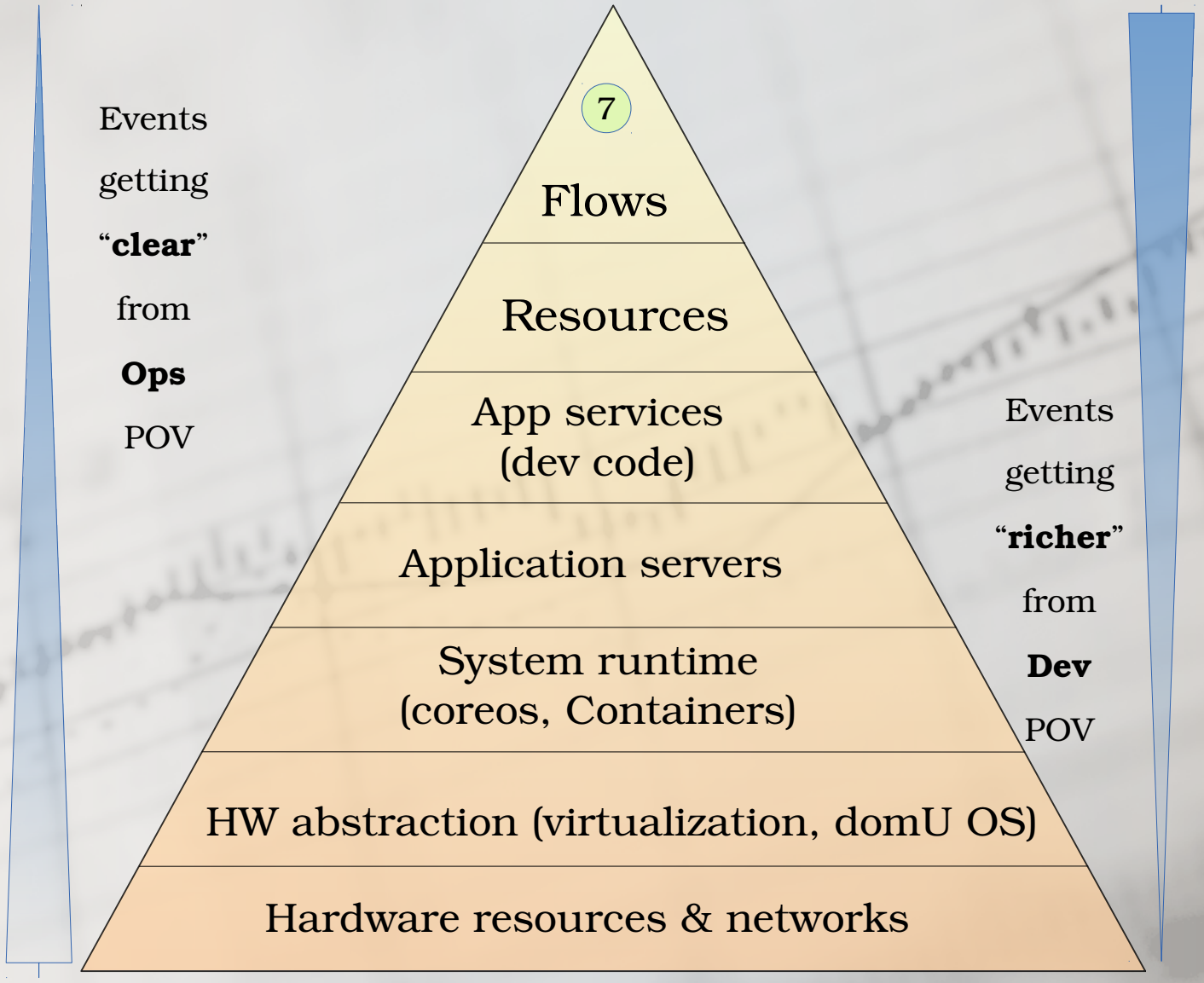
Green – CIO

Gray - Enterprise Architects

Blue – PMO

Orange – IT service production

What's wrong: “rich” vs “clear”



The game)

What is wrong with monitoring & logging now?

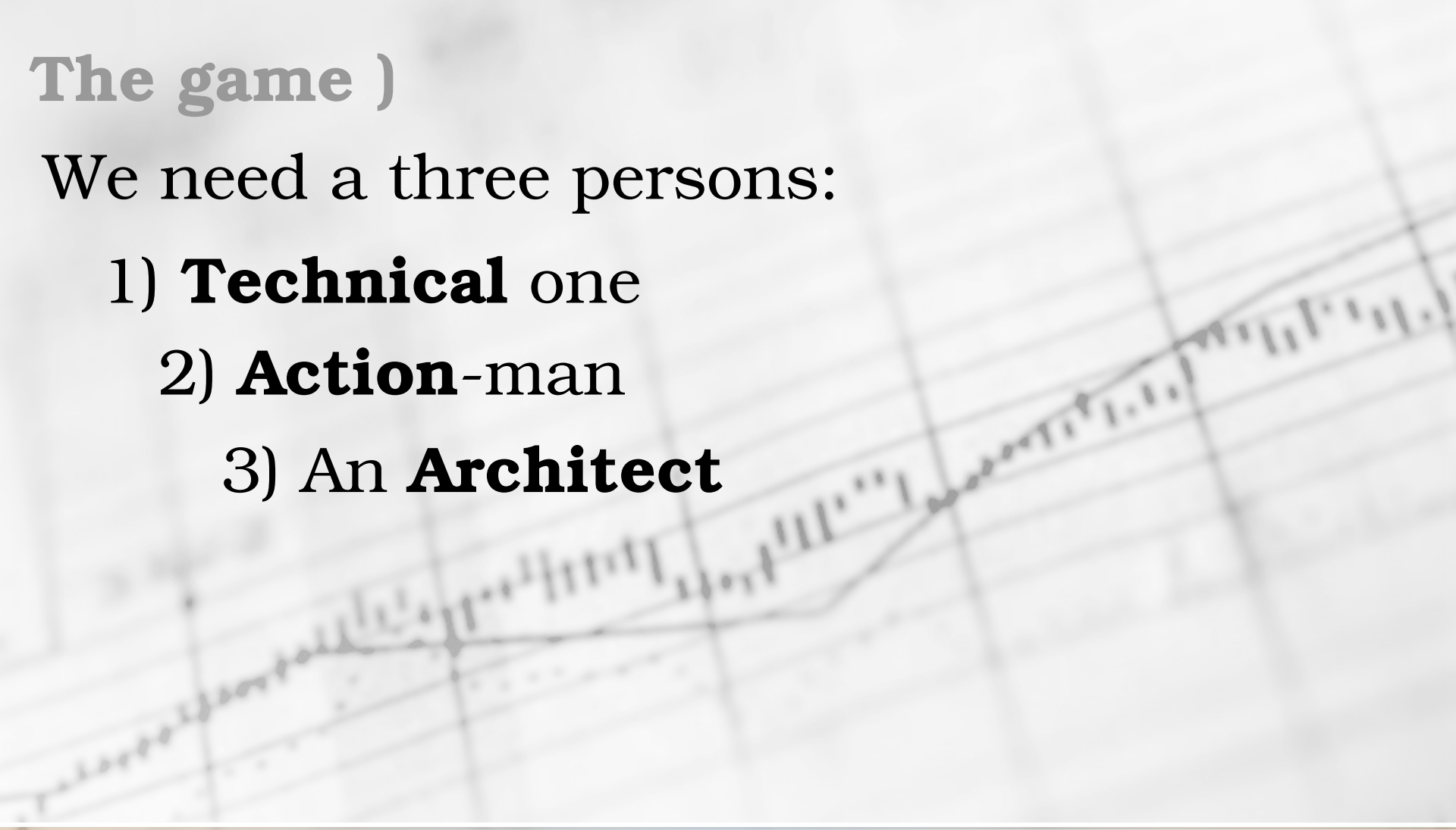
The game)

We need a three persons:

1) **Technical** one

2) **Action**-man

3) An **Architect**



What is wrong with monitoring & logging now?

The game)

We need a three persons:

1) **Technical** one

2) **Action**-man

3) An **Architect**

Time mashine moving us to 2025

Beep – beep – beeeeep… moving to the future

The game)

In 2025

We need a three persons:

1) **Technical** one

2) **Action**-man

3) An **Architect**

The questions from 2025

1) **Please describe a successful** monitoring-like solutuion

The game)

In 2025

We need a three persons:

1) **Technical** one

2) **Action**-man

3) An **Architect**

The questions from 2025

2) **How we will use** monitoring-like solutions in 2025?

The game)

In 2025

We need a three persons:

1) **Technical** one

2) **Action**-man

3) An **Architect**

The questions from 2025

3) **Describe a value** of monitoring-like solutions for end users/IT/business

The game)

What is wrong with monitoring & logging now?

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

What is #architecture-driven logitoring lifecycle?

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

Best practices:

1) self-reported status

(**systemd integration** as example)

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

Best practices:

1) self-reported status

(**erlang zabbix sender** as example)

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

Best practices:

1) self-reported status

(**haproxy syslog** as example)

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

Best practices:

1) self-reported status

(**exim syslog** as example)

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

Best practices:

2) dynamic items

(**Zabbix LLD** as example)

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

Best practices:

2) dynamic items

(**Elasticsearch & Kibana4** as example)

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

How we can integrate Archi-schemes in Zabbix?

(maps)

Logitoring

Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

How we can integrate Archi-schemes in Zabbix?

(item/trigger source)

Logitoring

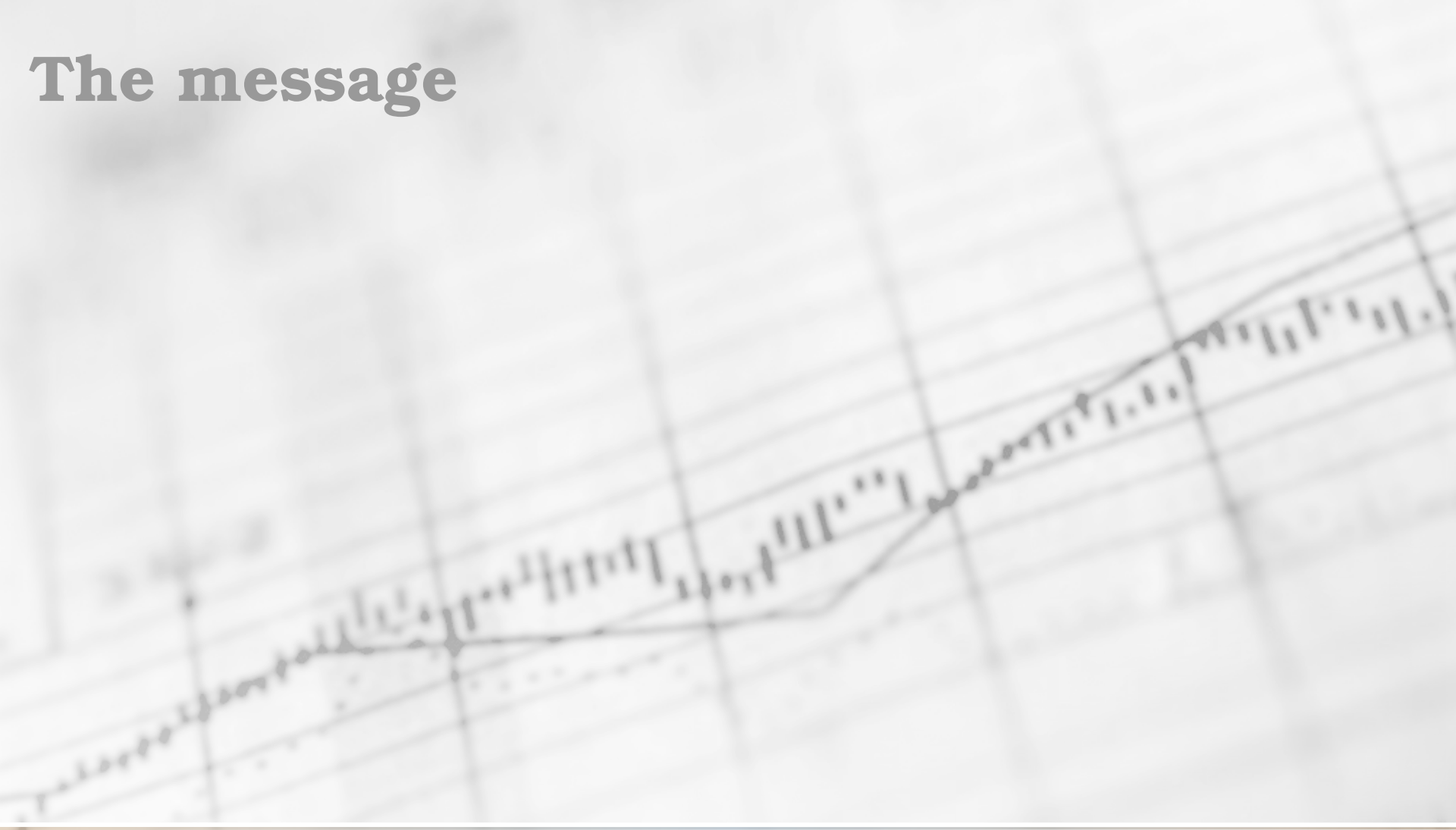
Architecture-driven logitoring lifecycle

"The matter of logitoring is events/facts provision to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore - Both are just the functions of the event provision engine"

How we can use Archi-schemes as CMDB/Service Registration ?

The message



What I'm speaking about last 20 minutes?

The message

We need to cooperate

In order to build up

"The matter of logitoring
is events/facts provision
to all infrastructure levels.

There are no "logging" or "monitoring" terms anymore -
Both are just the functions of the event provision engine"

the successful monitoring-like solutuion
reflecting our real business value

Thanks!

Architecture-driven

logitoring lifecycle

or

"please, no more another
ugly DevOps logging and monitoring pattern"

the meaning of "logitoring" in architecture-driven logitoring lifecycle

[please relax, take a deep breath

and feel free to speak about :]

Thanks!

Architecture-driven logitoring lifecycle

or

"please, no more another
ugly DevOps logging and monitoring pattern"

the meaning of "logitoring" in architecture-driven logitoring lifecycle

Eugene Istomin
IT Architect

e.istomin@edss.ee
Cone Center,Tallinn