Internet of Things: Technical Approaches towards Sustainability

Ringvorlesung Nachhaltigkeit, Universität Bremen, 2023-12-18

https://slides.cabo.space

Prof. Dr.-Ing. Carsten Bormann, cabo@tzi.org

Carsten Bormann

Universität Bremen TZI
IETF CoRE WG
IRTF T2T RG

https://slides.cabo.space

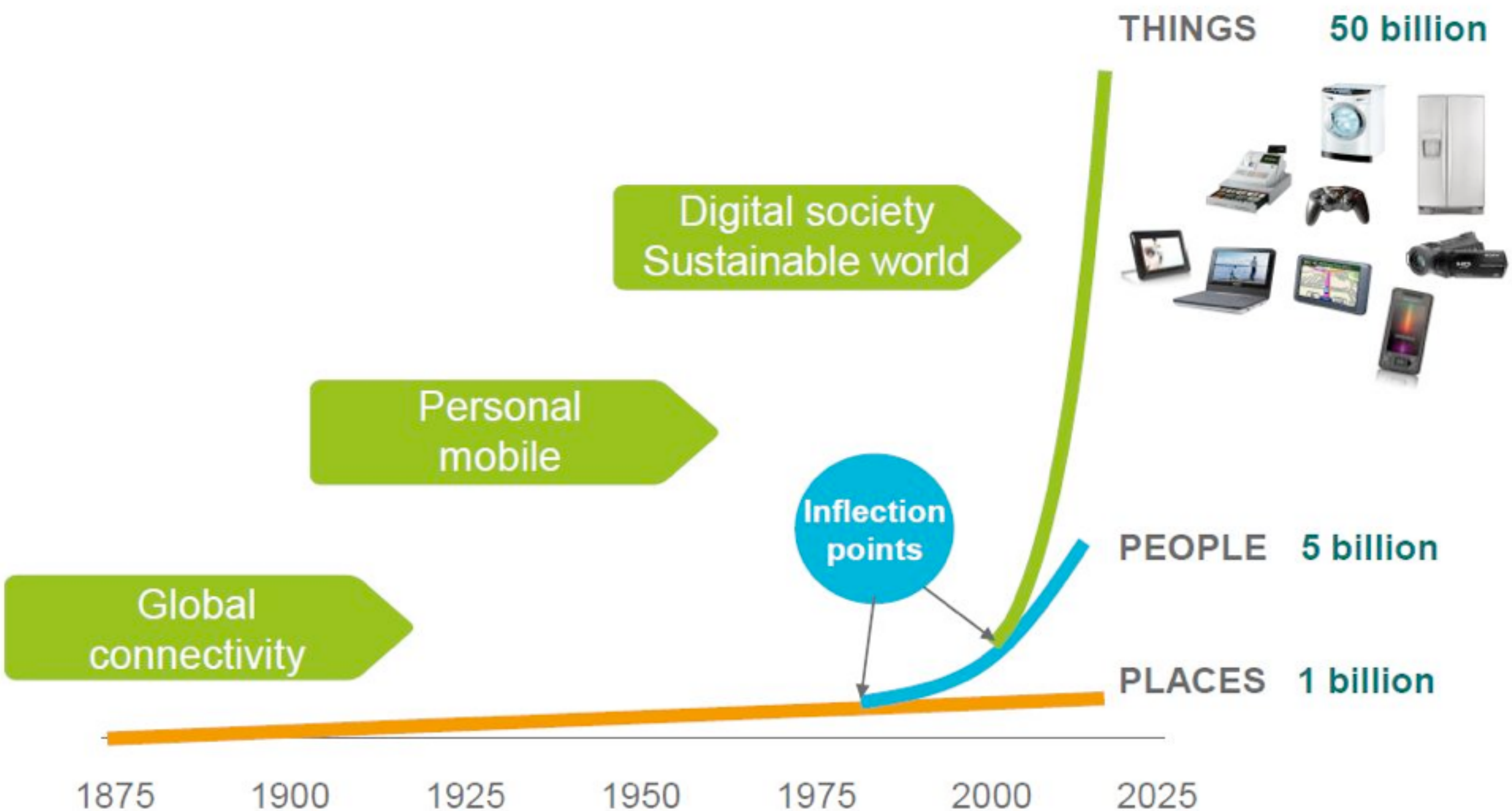
Carsten Bormann: Abbreviated bio 🤓

RFC 2429	RFC 2509	RFC 2686	RFC 2687	RFC 2689	RFC 3095	RFC 3189
RFC 3190	RFC 3241	RFC 3320	RFC 3485	RFC 3544	RFC 3819	RFC 3940
RFC 3941	RFC 4629	RFC 5049	RFC 5401	RFC 5740	RFC 5856	RFC 5857
RFC 5858	RFC 6469	RFC 6606	RFC 6775	RFC 7049	RFC 7228	RFC 7252
RFC 7400	RFC 7959	RFC 8132	RFC 8138	RFC 8307	RFC 8323	RFC 8428
RFC 8610	RFC 8710	RFC 8742	RFC 8746	RFC 8798	RFC 8930	RFC 8949
RFC 8990	RFC 9090	RFC 9100	RFC 9164	RFC 9165	RFC 9176	RFC 9193
RFC 9202	RFC 9237	RFC 9254	RFC 9277	RFC 9290	RFC 9485	jsonpath-base
core-target-attr	datetime-extended	cbor-time-tag	…			

Bringing the Internet to new applications

- "Application X will **never** run on the Internet"
- …
- …
- "How do we turn off the remaining parts of X that **still** aren't on the Internet"?

Connecting:
Places → People → Things



Source: Ericsson

Thingness

A "**Thing**" in the Internet of Things is:

- connected to a network, providing **digital** affordances (interaction opportunities)
- connected to the **physical** world, sensing and actuating (also: displaying)

Why IoT

- For humans, IoT can
  - **increase comfort**
  - **save time**
  - **save cost**
- IoT can help **save resources**
- IoT **consumes resources**
  - One-time: production, installation, disposal
  - Continuous: operation

Internet of Things

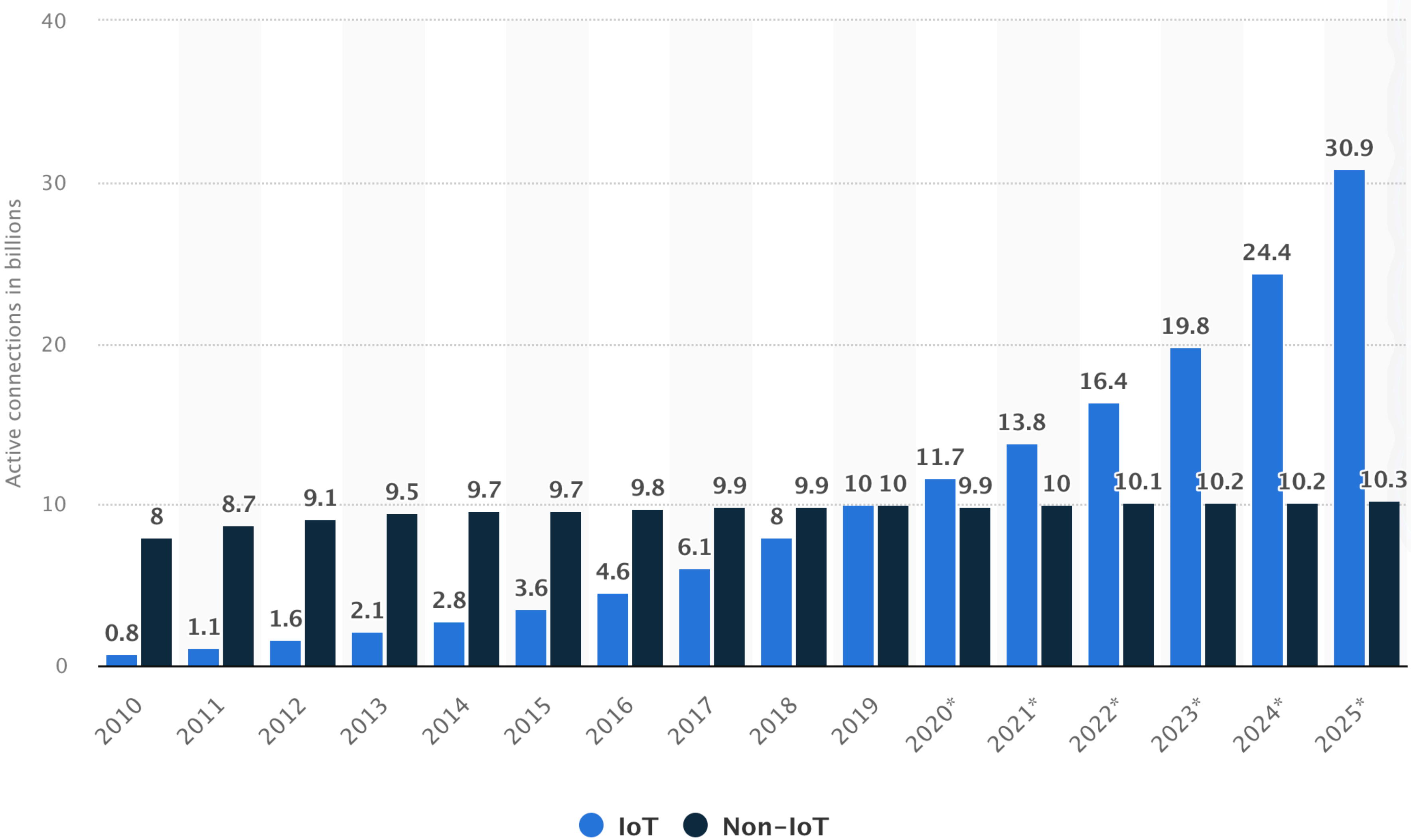
Scale up:

Number of nodes

(xx billion by 202x)

https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

Internet of Things (IoT) and non-IoT active device "connections" worldwide from 2010 to 2025 (billions)



Internet of Things

Scale down:

node

Internet of Things

Scale down:

cost

complexity

cent
kilobyte
megahertz

Constrained nodes: orders of magnitude

10/100 vs. 50/250

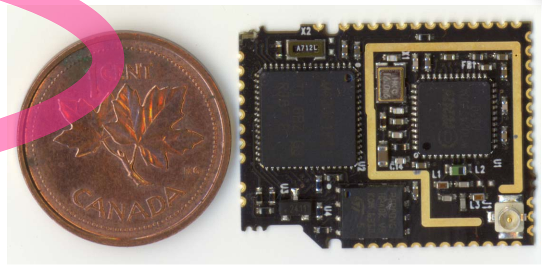
There is not just a single class of "constrained node"

RFC 7228

Class 0: too small to securely run on the Internet
- ✘ "too constrained"

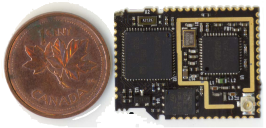
Class 1: ~10 KiB data, ~100 KiB code
- ✔ "quite constrained", "10/100"

Class 2: ~50 KiB data, ~250 KiB code
- ✔ "not so constrained", "50/250"



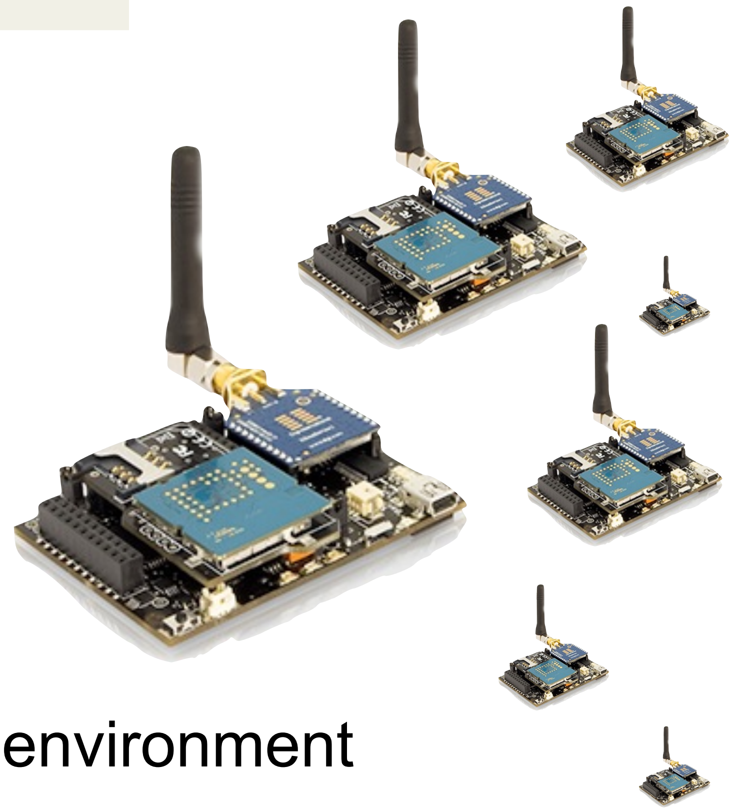
These classes are not clear-cut, but may structure the discussion and help avoid talking at cross-purposes

http://www.flickr.com/photos/blahflowers/3878202215/sizes/l/



http://www.flickr.com/photos/blahflowers/3878202215/sizes/l

Constrained **networks**



- **Node**: ... must sleep a lot (**µW**!)
  - vs. “always on”
- **Network**: ~**100 kbit/s**, high loss, high link variability
- May be used in an unstable radio environment
- Physical layer packet size may be limited (~**100 bytes**)
- “LLN low power, lossy network”

802.15.4 „ZigBee“
Bluetooth Smart
Z-Wave (G.9959)
DECT ULE

Constrained Node Networks

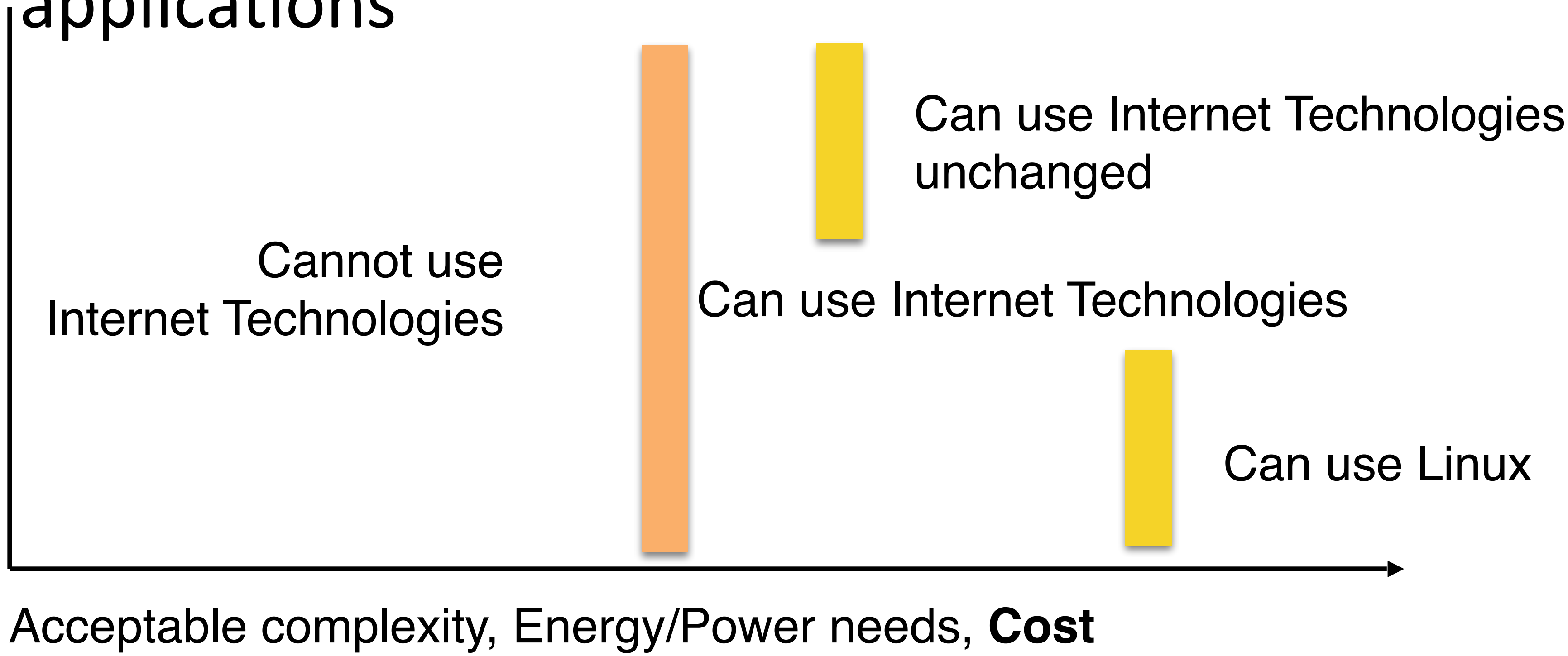
Networks built from
Constrained Nodes,
where much of the
Network Constraints come from
the constrainedness of the Nodes

in constrained node/networks, **Moore's law barely applies**

- In the low-power, low-cost area, gains from Moore's law are used
  - to save **power**
  - to save **cost**
- Performance, ROM, RAM grow **very** slowly

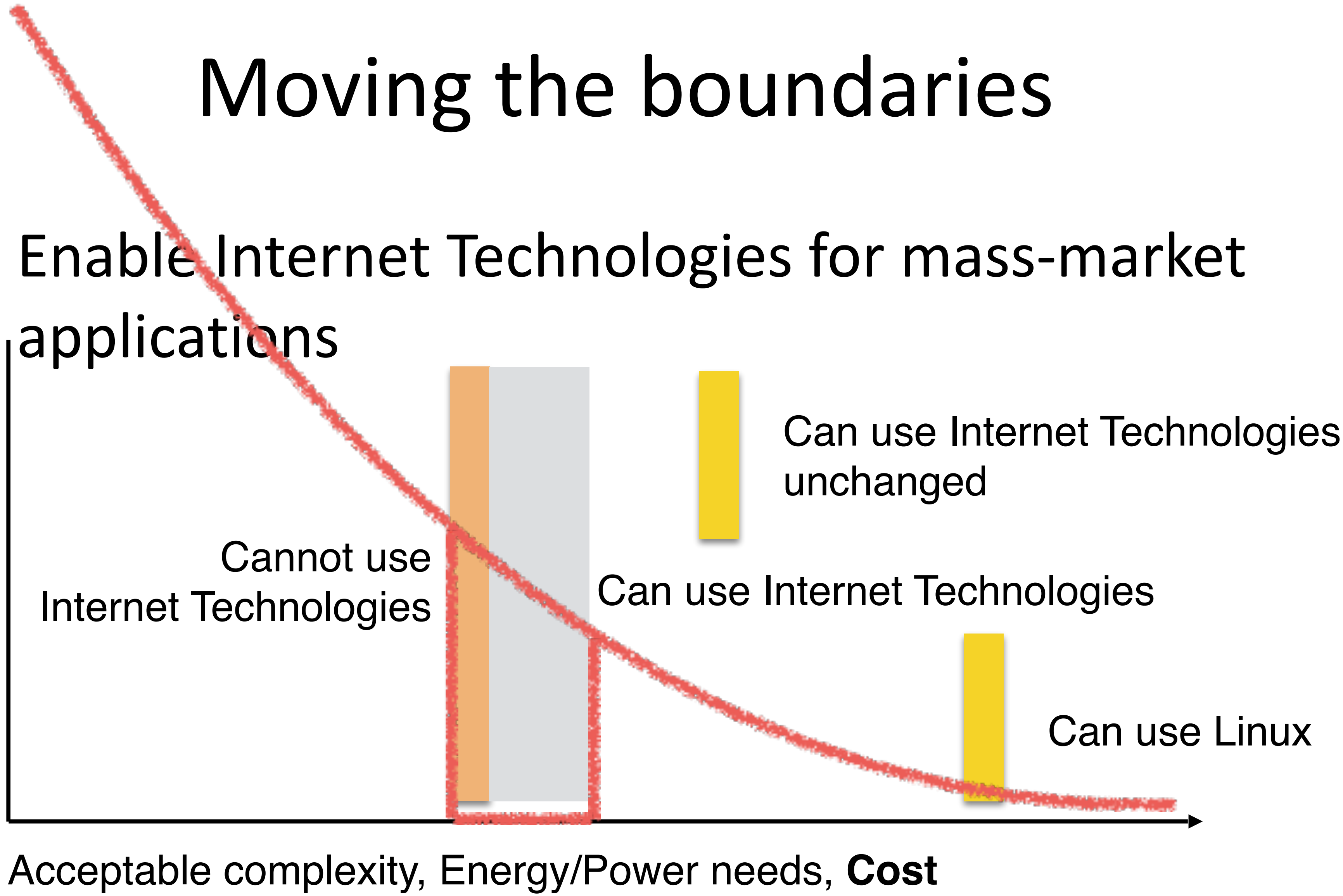
Moving the boundaries

- Enable Internet Technologies for mass-market applications



Moving the boundaries

- Enable Internet Technologies for mass-market applications



approaches

- some protocols can be **fixed**
  - ND ➻ 6LoWPAN-ND

= retargeted for less generality, more austerity

- some protocols can be re-used after **removing sources of complexity**
  - e.g., DTLS without X.509
- some **architectures** can be re-used with more appropriate protocols
  - e.g., reincarnate HTTP's REST in CoAP

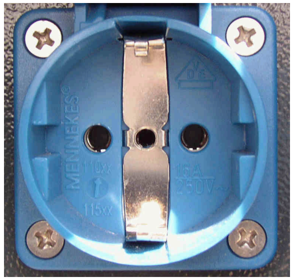
Resource Use:
Energy Consumption

What is a **Watt**?

- **Power**:
  1 Watt = 1 Newton × 1 Meter = 1 Volt × 1 Ampere (ISO 80000, SI)

- **Energy**:
  1 Watt × 1 Second = 1 Joule (J)
  1000 Watt × 3600 Seconds = 1 kWh ≅ 0.40 €
  1 Watt × 1 Year = 1 W × 8760 h = 8.76 kWh ≅ **3.50 €**

  1 Watt × 1 Year = 8.76 kWh ≅ **0.5 kg CO_2 (France)**
  1 Watt × 1 Year = 8.76 kWh ≅ **2.9 kg CO_2 (Germany)**
  1 Human Body x 1 Year ≅ 200–300 kg CO_2
  1 per-Human Consumption x 1 Year ≅ 4000–16000 kg CO_2



Off-grid:
Using primary batteries?

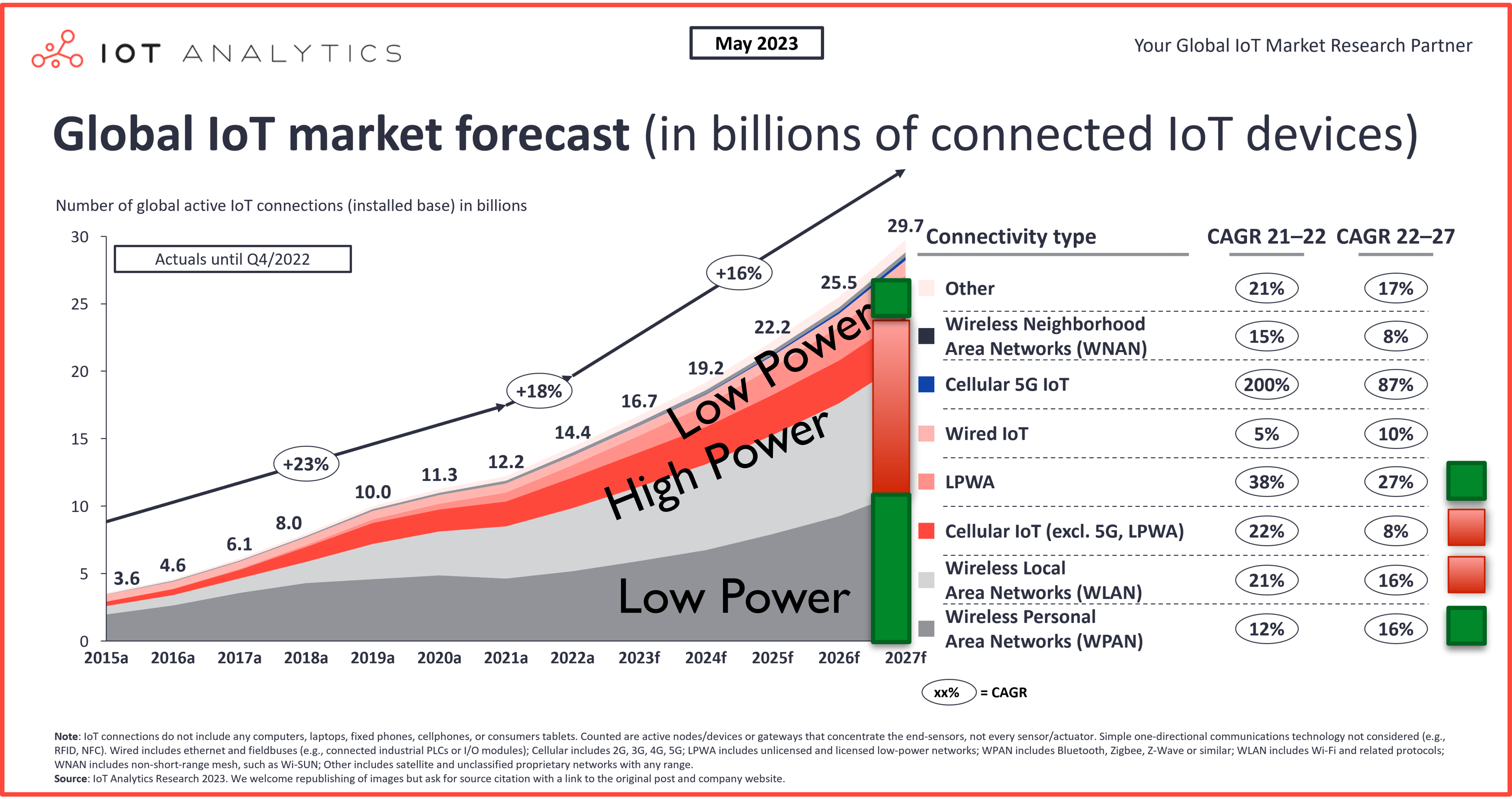
- Example: AA cell (LR6), VARTA Industrial:
  - ~ 2.7 Wh (0.0027 kWh)
  - € 0.30 bulk consumer price

- 111 €/kWh ≅ **1000 €/Watt-year**
- 0.107 kg CO_2 per cell (material, manufacture, transport)[1]
  350 kg CO_2 per Watt-year

[1] Ramsey Hamade et al.
Life Cycle Analysis of AA Alkaline Batteries
Procedia Manufacturing 43 (2020) 415–422

Hype-IoT	Real IoT
IPv4, NATs	IPv6
Device-to-Cloud	Internet
Gateways, Silos	Small Things Loosely Joined
Questionable Security	Real Security
$40+	< $5
W	mW, μW

“Connected” IoT Devices



https://iot-analytics.com/wp/wp-content/uploads/2023/05/Global-IoT-market-forecast-in-billions-of-connected-IoT-devices.png

IETF®

Disclaimer (IETF/IRTF)

- Nobody speaks for the IETF
  - The IETF is a collection of consensus processes
- Formal Liaisons are managed by the IAB

IETF: Constrained Node Network WGs

INT	LWIG	Guidance
INT	6LoWPAN ✔	IP over 802.15.4
INT	6Lo	IP-over-foo
INT	6TiSCH	IP over TSCH
INT	LPWAN	Low-Power WAN Networks
RTG	ROLL	Routing (RPL)
APP	ASDF ♨	Semantic Description
APP	CoRE	REST (CoAP) + Ops
APP	CBOR	CBOR & CDDL
SEC	DICE ✔	Improving DTLS
SEC	ACE	Constrained AA
SEC	COSE	Object Security
SEC	LAKE	Key Agreement (Handshake)
SEC	SUIT ♨	Software Update
SEC	RATS ♨	Attestation
OPS	IOTOPS ♨	Operations

Application Layer Protocols

- CoRE: Constrained **REST**ful Environments:
  Replace HTTP by a less expensive equivalent (**CoAP**)
    - From special-purpose/siloed to **general purpose**
- ACE: Define **Security** less dependent on humans in the loop and on very fast upgrade cycles
    - Embrace the **multi-stakeholder** IoT

Application Layer
Data Formats

- Industry move to **JSON** for data interchange
- Add **CBOR** where JSON is too expensive
- Use **JOSE** and **COSE** as the security formats
- Work on semantic interoperability (IRTF **T2TRG**), with W3C, OCF, OMA/IPSO (LWM2M), iot.schema.org, …
  ➔ **self-description**

2013-09-13: CBOR

- **CBOR**: “Concise Binary Object Representation”
  RFC ~~7049~~ 8949 — JSON equivalent for constrained nodes
  - start from JSON data model (no schema needed)
  - add binary data, extensibility (“tags”)
  - concise binary encoding (byte-oriented, counting objects)
  - add diagnostic notation
- Started AD-sponsored, turned into a WG on 2017-01-09
- **CDDL**: Description language for CBOR (and JSON): RFC 8610

https://youtu.be/y46dARLUmmI

Data Formats

	Character-based	Concise Binary
Document-Oriented	XML	EXI
Data-Oriented	JSON	???

	Character-based	Concise Binary
Document-Oriented	XML	EXI
Data-Oriented	JSON	CBOR

CBOR vs. "binary JSONs"

- Encoding [1, [2, 3]]:   compact | stream

```
ASN.1 BER*    | 30 0b 02 01 01 30 06 02 | 30 80 02 01 01 30 06 02
              | 01 02 02 01 03          | 01 02 02 01 03 00 00
              |                         |
MessagePack   | 92 01 92 02 03          |
              |                         |
BSON          | 22 00 00 00 10 30 00 01 |
              | 00 00 00 04 31 00 13 00 |
              | 00 00 10 30 00 02 00 00 |
              | 00 10 31 00 03 00 00 00 |
              | 00 00                   |
              |                         |
UBJSON        | 61 02 42 01 61 02 42 02 | 61 ff 42 01 61 02 42 02
              | 42 03                   | 42 03 45*
              |                         |
CBOR          | 82 01 82 02 03          | 9f 01 82 02 03 ff
```

Object Security Standards

Format	Basis	Who	Where
CMS	ASN.1	RSA, IETF	S/MIME
XMLDSig	XML	W3C, IETF	SOAP*
JOSE	JSON	IETF	Web
COSE	CBOR	IETF	IoT

Selecting data representation formats for reduced energy

Brendan Moran, Henk Birkholz, Carsten Bormann

CBOR is Greener than JSON

IAB e-impact Workshop (submitted 31 October 2022)

Does encoding matter?

Why optimize if the difference is small?

Data impacts on encoding size

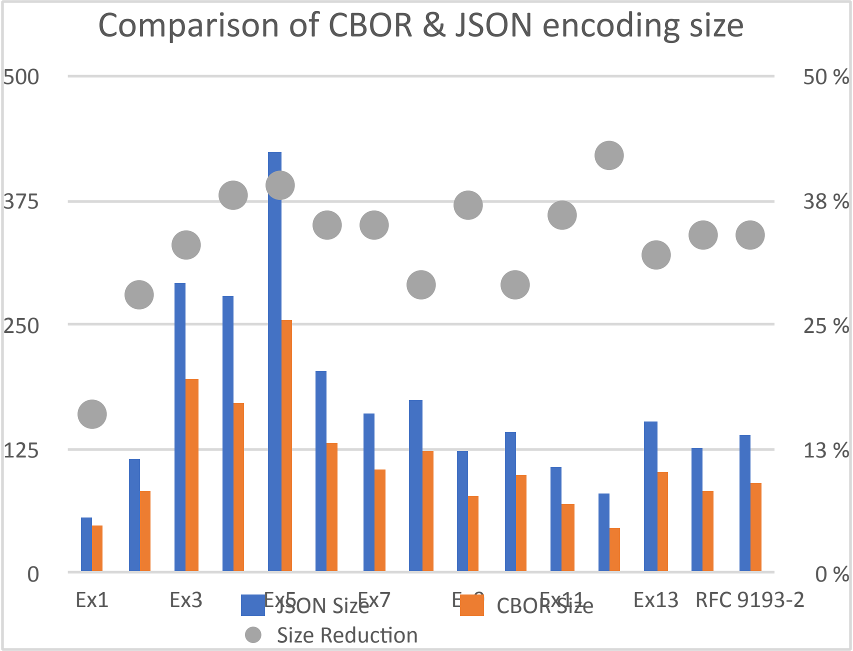
- Text data encodes into text formats well.
  - Non-text encodes poorly
  - Hex escape sequences produce 4x inflation of escaped octets
- Binary data encodes into text formats poorly:
  - Base64 = 33% data inflation
- Integers encode poorly into text
  - Typically 50% data inflation
- Floating point encodes poorly into text
  - Trivial examples are smaller than binary (e.g. 1.1)
  - Real examples are larger than binary (e.g. -1.01)
- Structures encode poorly into text
  - Separators, beginning and end markers are needed
  - Data inflation typically 2 + N – 1 for N elements (e.g. JSON)

Type	JSON Size	CBOR Size
string	strlen+2 + escaping	strlen + UINT(strlen)
octets (hex)	bytesize * 2	bytesize + UINT(bytesize)
octets (b64)	bytesize * 4/3	bytesize + UINT(bytesize)
int8	1 to 3	1 or 2
int16	1 to 5	3
int32	1 to 10	5
int64	1 to 19	9
float32	3 to 16	5
float64	3 to 23	9
Date	12	2 + UINT(days since 1970)

Practical differences in encoding data size

Size comparison of JSON vs CBOR in SenML Examples

- Data from SenML examples
- Encoded as both JSON and CBOR
- CBOR size reduction in all cases
  - Often 33% or better



SenML Example	JSON Size	CBOR Size	Size Reduc
Ex1	56	47	16%
Ex2	115	82	28%

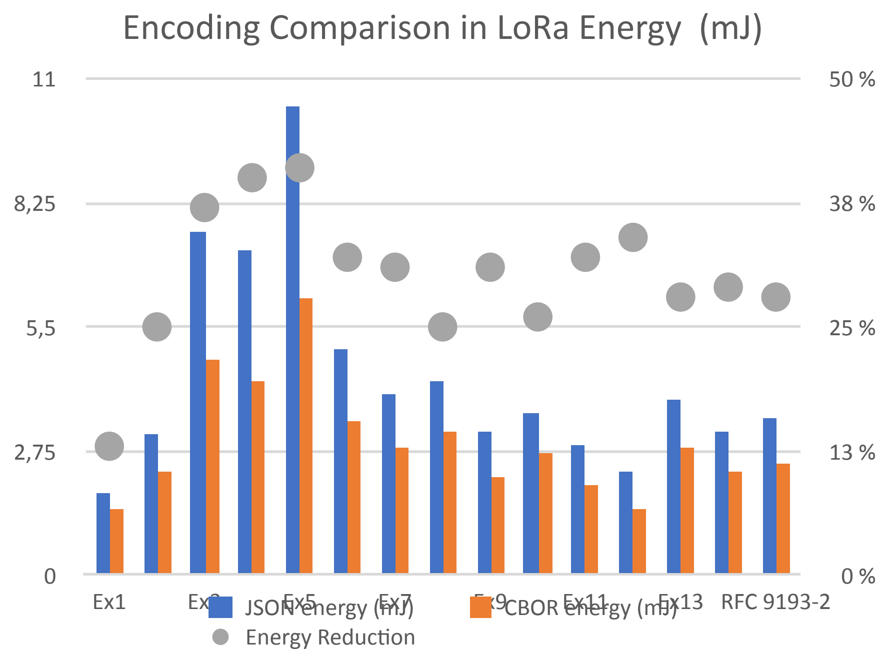
Encoding impact on energy

Why optimize if energy impact is small?

Energy impact of data size by encoding

Energy comparison of JSON vs CBOR in SenML Examples

- LoRa overhead reduces impact
  - Sensitive to packet count
  - Quantized to 127 bytes
  - Per-packet overhead
    - Favors reduction across packet count
- Energy reduction in all cases
  - Often 30% or better



SenML Example	JSON energy (mJ)	CBOR energy (mJ)	Energy Reduct
Ex1	1.8	1.5	13%
[illegible]	[illegible]	[illegible]	[illegible]

Impact of energy reduction in constrained networks

- Smaller batteries
- Longer life
- Smaller need for energy harvesting
- Reduced e-waste (for primary cell)
- Lower cost

Encoding Choices in IETF

JSON & CBOR account for most hierarchical data formats

Common myths of text formats

Why people still think they like text formats

- “It’s easier to debug JSON”
  - Many tools for CBOR ➔ CBOR Debug
- “I don’t need to install a tool to look at JSON”
  - CBOR decoding can be done in a web browser

Unpleasant truth:

- These are tooling problems, not encoding problems.
- The vast majority of traffic is never debugged.
- Plan for primary use case: machine interpretation

Benefits of binary encodings

- Simple to parse
    - Low embodied energy
        - Low code
        - Low memory
    - Low active energy
        - Low compute overhead
- **Lower data use**
    - Lower transmit & receive energy
- Lower interpretation complexity
    - Simpler security posture
- **Less per-character work**
    - Escaping, delimiting
- **Less redundant conversion work**
    - Decimal conversion
    - Base64 encoding
- More deterministic
    - Whitespace
    - Escape choices

Recommendations

Suggestions to the IAB

- Consider content and intended use for data representation formats:

Configuration documents	Text formats are appropriate
Primarily text content	Text formats are appropriate
Primarily non-text content	**Binary formats should be preferred**

- Not a game changer for e-impact, but a small contribution

Premature optimization
is the root of all evil.

Donald Knuth, Structured Programming With Go To Statements
Computing Surveys, Vol 6, No 4, December 1974

Absolute Statements
are the root of all evil.

C2 Wiki

Don't pessimize prematurely.
(Avoiding premature optimization ≠ gratuitously hurting efficiency.)

Herb Sutter, C++ Coding Standards (paraphrased)

Classes of Energy Limitation

- E0–E2: Hard limits; constrained device
- E9: No *limits*, but can we still reduce energy use?

  Adopt IoT-oriented developments in "mainstream"?

Name	Type of energy limitation	Example Power Source
E0	Event energy-limited	Event-based harvesting
E1	Period energy-limited	Battery that is periodically recharged or replaced
E2	Lifetime energy-limited	Non-replaceable primary battery
E9	No direct quantitative limitations to available energy	Mains-powered

Table 6: Classes of Energy Limitation

https://www.ietf.org/archive/id/draft-ietf-lwig-7228bis-00.html#power

Layer 2: Energy-efficient Ethernet

- Ethernet-Port consumes power when “on” (ready for data transfer = data transfer active)
- Energy Efficient Ethernet (EEE) standard (IEEE 802.3az): **Low-Power Idle** ➔ wakeup adds small latency
- **Adaptive Link Rate** (ALR): Switch speeds ➔ adds more latency
- Upgrade cost: Included in chip!

Table III. Baseline power consumption values.

Link speed	Active state	Low-power state (10%; mW)	Power/Mbps at full load (mW/Mbps)
100Base-TX	200 mW	20	2
1000Base-T	600 mW	60	0.6
10GBase-T	4 W	400	0.4

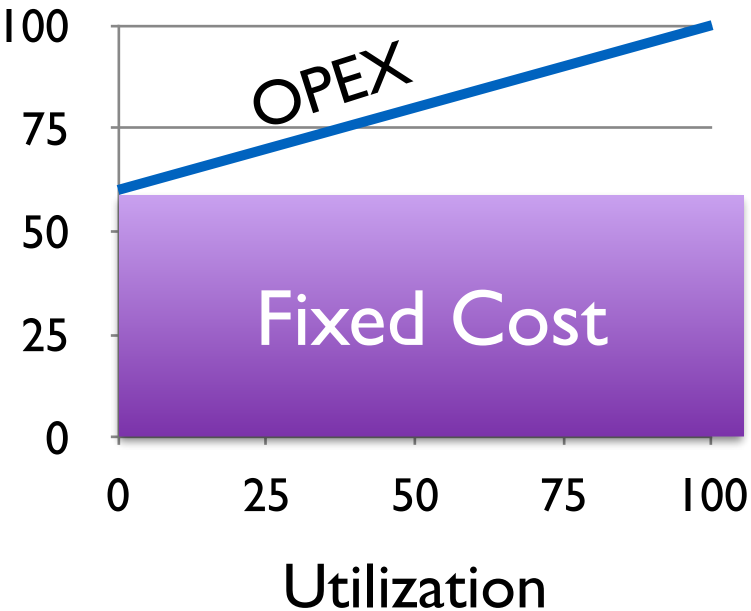
P. Reviriego, J. A. Maestro, J. A. Hernández and D. Larrabeiti
Study of the potential energy savings in Ethernet by combining Energy Efficient Ethernet and Adaptive Link Rate
Trans. Emerging Tel. Tech. 23 (2012) 3, pp. 227-233, DOI:10.1002/ett.1526

Layer 3: Efficient ND

- IPv6 Neighbor discovery (ND): based on Multicast
  - Ethernet assumption:
    inexpensive to **ask everyone**
- RFC 6775 (2012): 6LoWPAN-ND
  rethink IPv6 for low-power WPAN (IEEE 802.15.4):
  - Replace multicast by designated node (6LBR)
- "efficient ND": Adapt 6LoWPAN-ND for Ethernet
  - Fewer wakeups of links and hosts
  - Upgrade cost: large inertia

Cost of running a service

- **CAPEX** (Capital Expenditure): initial investment
  - Amortizes over life time
- **OPEX** (Operational Expenditure): running cost
  - Fixed cost:
    - Providing Capacity
    - Keeping Attention (Management)
  - Variable cost: (resource use increases with utilization)

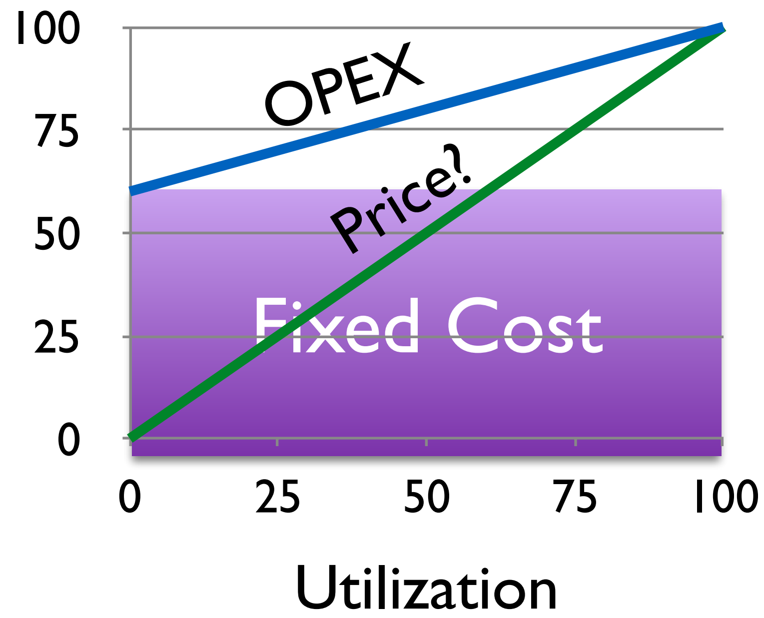


What do people pay for?

- Per-usage cost (“**metering**”)
  - Deters from each individual usage
    ➔ capacity often sits idle
  - Does not pay for fixed OPEX or CAPEX
- Fixed cost (“**flat rate**”)
  - Market differentiation via amount of capacity rented

Attribution of Resource Usage

- Fixed Costs Include Prices on Fixed Resource Usage (e.g., CO_2 price for keeping system running)
- Who "pays for" fixed costs?



Utilization incentives

- Metered cost: “I don’t need this right now”
  ➔ utilization stays low ➔ usage stays expensive ➔
- Flat rates: “already paid”
  ➔ opportunities for deriving benefit are actually used
  - Utilization increases until capacity ceiling is hit
- Stairstep effect of “flat rates”:
  - Add capacity in steps, often technology motivated
  - “Forklift paradox”:
    Replacing systems **increases** efficiency
    (vs. “rebound effect”)

Resource Use:
Device Waste

One-time cost:
Consumed materials + embodied energy

End of amortization period:

- No longer needed — can it be **reused**?
- Defective hardware — can it be **repaired**?
    - Defective software — can it be **upgraded**?
- Replacement by "better" device
    - Better technology
    - Level-up class: more justified usage
    - Can it be **upgraded** ➔ lower cost, less waste
- No longer supported (cloud side, app, security)
  — can it be **retargeted**?

IoT Device lifecycle

Garcia-Morchon, et al.   Informational   [Page 6]

RFC 8576   IoT Security   April 2019

```
 _Manufactured           _SW update          _Decommissioned
/                       /                   /
|   _Installed          |   _ Application   |   _Removed &
|  /                    |  / reconfigured   |  /  replaced
|  |   _Commissioned    |  |                |  |
|  |  /                 |  |                |  |   _Reownership &
|  |  |    _Application |  |   _Application |  |  / recommissioned
|  |  |   /   running   |  |  / running     |  |  |
|  |  |   |             |  |  |             |  |  |             \\
+##+##+###+#############+##+##+#############+##+##+###############>>>
    \/  \______________/ \/  \_____________/ \___/         time //
    /           /         \          \          \
Bootstrapping  /      Maintenance &   \     Maintenance &
              /      rebootstrapping   \   rebootstrapping
        Operational                Operational
```

Figure 1: The Lifecycle of a Thing in the Internet of Things

Software Upgrades?

- Supply more functionality
- Mend functional defects (crashes, broken function)
- Mend security defects
  - Impacting the IoT use:
  - Impacting third parties:
    IoT Devices as an **attack platform**
- Defuse time bombs (certificates!)
- Exit vendor ecosystem (retarget)
  - Vs. take-over by attacker

Operating a dangerous device?

Device can do third-party damage
➔ Liability! (Compare: electrical devices, cars, …)

- **Owner/operator duty**?
  - Delegation? (cf. Garage)
- **Vendor duty**?
  - Regulation?
  - Self-certification?

Software Updates are needed

- Bugs are being found
- Environments change

→ **Update or discard!**

- Traditional: manual upgrade by connecting a special upgrader device (e.g., PC with upgrader app)
    - Too expensive; device might be hard to reach
- Needed: **Secure** Over-the-air Upgrade
- IETF SUIT WG — manifest format for updates

2017-12-15: SUIT

- “Software Updates for Internet of Things”
- Signed **manifest** describes software update
  - Enables device to decide whether to accept it
- SUIT: Information model, architecture, **manifest format**
- Based on CBOR, COSE; described in CDDL

Manufacturer's Usage Description (MUD)

- Protect the network and other **unrelated** users against an IoT Device that may be insecure
- Idea: Document **expected behavior** in an actionable way
- MUD as standardized today (**RFC 8520**): Can be used for **firewall** configuration
  - Poke firewall holes for desirable traffic
  - **Detect** when the IoT Device has been compromised
- Where can we take this idea?

Is my device vulnerable?

- CVE: Common Vulnerabilities and Exposures

Thousands of software components: Managing the Supply Chain

- ♨ SBOM: Software Bill of Materials
- ♨ Signed **transparency** logs (SCITT)

2019-03-07: RATS

- Beyond *Dolev-Yao*:
  Securing the Communication is not enough
- What do we know about that security status of a host?
- **RATS** = Remote Attestation Procedures
  (Not just for IoT!)
- Conveying and Appraising Evidence:
  - (1) describing assertions/claims about system components and associated evidence
  - (2) procedures and protocols to convey these assertions/ claims to relying parties

If it is not **usably secure**,
it's not
the **Internet of Things**

Resource Use:
Incentives and Disincentives

Deployment Economy

- Deployment:
  Need to get all parties on board that need to act
- Benefits need to accrue where the cost is spent
- Innovation is risk taking: Rewards needed

Rewards/Incentives?

- Natural Incentives
  - Save cost, reduce **risk**
  - Derive additional benefit (profit)
- Increase Goodwill (Marketing)
  - Organize quality marks, voluntary certification
- Remove Obstacles/Risks
  - Create **standards** where needed
- Regulation
  - Subsidies for compliant behavior
  - Prohibition of non-**compliant** business

I E T F®